

Deepfake sebagai Kejahatan Siber Kontemporer: Kajian Yuridis Normatif atas Kelemahan Konstruksi Hukum Pidana Indonesia dan Urgensi Reformasi Legislatif

Ubaidila

Fakultas Hukum Ilmu Politik, Program Magister Ilmu Hukum, Universitas Muhammadiyah
Surakarta, Indonesia
Ubaiddazi@gmail.com

Izzul Fikri Arif Tamamy

Fakultas Hukum Ilmu Politik, Program Magister Ilmu Hukum, Universitas Muhammadiyah
Surakarta, Indonesia
ariftamamyizzulfikri@gmail.com

Abstract. The rapid proliferation of deepfake technology poses unprecedented threats to Indonesia's criminal justice system, particularly in light of the new Criminal Code (KUHP) enacted through Law No. 1 of 2023, which came into force on 2 January 2026. This normative juridical study examines two interrelated questions: (1) what specific characteristics distinguish deepfake crimes from other forms of cybercrime, thereby requiring a specialised criminal law approach and (2) whether the normative constructions of the old and new Criminal Codes are adequate to address deepfake crimes, and if not, how such gaps should be resolved. Employing doctrinal legal analysis through grammatical, systematic, and teleological interpretation of primary legal materials, this study identifies critical normative deficiencies in both instruments. The old Criminal Code suffers from definitional limitations, a technological gap, and the absence of specific biometric manipulation regulations. While the new Criminal Code demonstrates significant progress expanding forgery to include electronic documents (Articles 252-253), regulating digital privacy violations (Articles 418-420), and criminalising non-consensual pornographic content (Articles 412-413) critical gaps persist: the absence of an explicit deepfake definition, ambiguity in classifying deepfake media as electronic documents, unclear biometric manipulation norms, and mens rea constructions inadequate for autonomous AI systems. The study recommends explicit legislative amendments with technology-neutral yet precise language, technical evidentiary guidelines for digital forensics, institutional capacity-building, comprehensive victim protection mechanisms, and digital literacy campaigns. Future research should empirically examine judicial application of these norms and test their effectiveness in Indonesian legal practice.

Keywords: deepfakes, criminal law, new Criminal Code, normative juridical, artificial intelligence

Abstrak. Penyebaran teknologi deepfake yang pesat menimbulkan ancaman yang belum pernah ada sebelumnya bagi sistem peradilan pidana Indonesia, khususnya dalam konteks Kitab Undang-Undang Hukum Pidana (KUHP) baru yang ditetapkan melalui Undang-Undang Nomor 1 Tahun 2023 dan mulai berlaku pada 2 Januari 2026. Penelitian normatif yuridis ini mengkaji dua pertanyaan yang saling berkaitan: (1) karakteristik spesifik apa yang membedakan kejahatan deepfake dari bentuk kejahatan siber lainnya sehingga memerlukan pendekatan hukum pidana yang khusus; dan (2) apakah konstruksi normatif dalam KUHP lama dan KUHP baru memadai untuk menangani kejahatan deepfake, dan jika tidak, bagaimana

kesenjangan tersebut harus diselesaikan. Dengan menggunakan analisis hukum doktrinal melalui interpretasi gramatikal, sistematis, dan teleologis terhadap bahan hukum primer, penelitian ini mengidentifikasi defisiensi normatif kritis pada kedua instrumen tersebut. KUHP lama memiliki keterbatasan definitif, kesenjangan teknologi, dan absennya regulasi manipulasi biometrik yang spesifik. Meskipun KUHP baru menunjukkan kemajuan signifikan memperluas konsep pemalsuan untuk mencakup dokumen elektronik (Pasal 252-253), mengatur pelanggaran privasi digital (Pasal 418-420), dan mengkriminalisasi konten pornografi tanpa persetujuan (Pasal 412-413) kesenjangan kritis masih ada: absennya definisi deepfake yang eksplisit, ambiguitas dalam mengklasifikasikan media deepfake sebagai dokumen elektronik, norma manipulasi biometrik yang tidak jelas, dan konstruksi mens rea yang tidak memadai untuk sistem kecerdasan buatan yang otonom. Penelitian ini merekomendasikan amandemen legislatif yang eksplisit dengan bahasa yang netral terhadap teknologi namun tepat secara hukum, pedoman pembuktian teknis untuk forensik digital, penguatan kapasitas kelembagaan, mekanisme perlindungan korban yang komprehensif, dan kampanye literasi digital.

Kata kunci: deepfake, hukum pidana, KUHP baru, normatif yuridis, kecerdasan buatan

PENDAHULUAN

Era digital kontemporer menghadirkan dilema paradoksal dalam peradaban manusia modern, di mana kemajuan teknologi kecerdasan buatan (AI) yang membawa transformasi revolusioner di berbagai aspek kehidupan sekaligus melahirkan ancaman baru dan fundamental terhadap fondasi kepercayaan sosial serta sistem hukum yang telah mapan. Salah satu manifestasi paling mengkhawatirkan dari evolusi teknologi AI adalah fenomena deepfake teknik manipulasi konten multimedia digital yang memanfaatkan algoritma pembelajaran mendalam untuk menghasilkan video, audio, dan gambar palsu dengan tingkat realisme yang sangat tinggi sehingga hampir tidak dapat dibedakan dari konten autentik¹. Teknologi ini telah berkembang secara eksponensial dan kini mudah diakses melalui aplikasi smartphone yang tersedia secara gratis, mengubah apa yang dulunya membutuhkan keahlian teknis tingkat tinggi menjadi kegiatan yang dapat dilakukan oleh pengguna biasa dalam hitungan menit².

Dampak destruktif dari penyalahgunaan teknologi deepfake telah terdokumentasi secara luas dalam literatur akademik, menggarisbawahi urgensi respons hukum yang komprehensif.³ menegaskan bahwa deepfake menimbulkan ancaman eksistensial terhadap tiga pilar fundamental masyarakat demokratis: kebenaran, kepercayaan, dan privasi. Data empiris

¹ Gilad Cohen and Raja Giryes, "Generative Adversarial Networks," in *Machine Learning for Data Science Handbook* (Cham: Springer International Publishing, 2023), 375–400, https://doi.org/10.1007/978-3-031-24628-9_17.

² Selvi Amelia, "Ruang Cyber vs Kebebasan Berpendapat : Menyeimbangkan Regulasi Dan Ekspresi Di Era Digital Banyak Manfaat Bagi Masyarakat , Terdapat Juga Kekhawatiran Yang Valid," *Staatsrecht Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024).

³ Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1753–1820, <https://doi.org/10.15779/Z38RV0D15J>.

menunjukkan bahwa jumlah video deepfake yang terdeteksi di internet meningkat drastis sebesar 550% antara tahun 2020 dan 2025, dengan proyeksi pertumbuhan yang terus berlangsung secara eksponensial seiring dengan demokratisasi akses terhadap teknologi AI generatif ⁴. Lebih mengkhawatirkan lagi, penelitian ⁵ mengungkapkan bahwa 96% konten deepfake yang beredar merupakan materi pornografi tanpa persetujuan, dengan mayoritas korban adalah perempuan yang wajahnya dimanipulasi tanpa izin dan disisipkan ke dalam konten pornografi, sehingga mengakibatkan viktimisasi digital yang parah dengan konsekuensi psikologis, sosial, dan ekonomi yang menghancurkan.

Di Indonesia, ancaman kejahatan deepfake semakin nyata dan mendesak, seiring dengan penetrasi internet yang mencapai 229,4 juta pengguna atau 80,66% dari total populasi pada tahun 2025 ⁶. Karakteristik unik masyarakat Indonesia yang ditandai oleh tingkat literasi digital yang relatif rendah di tengah penetrasi media sosial yang sangat tinggi menciptakan ekosistem yang sangat rentan terhadap penyebaran dan viktimisasi deepfake. Penelitian ⁷ menunjukkan bahwa Indonesia termasuk negara dengan tingkat penyebaran hoaks dan disinformasi tertinggi di Asia Tenggara, dan kemunculan teknologi deepfake berpotensi memperparah masalah ini secara signifikan, mengingat deepfake menghasilkan 'bukti visual' yang jauh lebih persuasif dan sulit dibantah dibandingkan hoaks tekstual konvensional.

Beberapa kejahatan terkait deepfake telah mulai teridentifikasi di Indonesia, meskipun statistik resmi yang komprehensif belum tersedia. Kasus yang terungkap mencakup manipulasi wajah tokoh publik untuk kepentingan propaganda politik menjelang pemilihan umum, pembuatan video pornografi palsu yang melibatkan selebriti dan influencer lokal yang kemudian disebarluaskan melalui platform media sosial, penggunaan audio deepfake untuk penipuan keuangan dengan meniru suara pejabat atau anggota keluarga korban, serta

⁴ Redaksi, "Deepfake Naik 550%, Platform Global Diminta Sediakan Fitur Cek Konten AI - Infodigital.Co.Id," accessed January 9, 2026, <https://infodigital.co.id/deepfake-naik-550-platform-global-diminta-sediakan-fitur-cek-konten-ai/>.

⁵ Henry Ajder et al., "The State of Deepfakes: Landscape, Threats, and Impact," 2019, <https://docslib.org/doc/12559428/the-state-of-deepfakes-landscape-threats-and-impact-henry-ajder-giorgio-patrini-francesco-cavalli-and-laurence-cullen-september-2019>.

⁶ APJII, "Survei Penetrasi Internet Dan Perilaku Penggunaan Internet Sebagai Perwakilan Pengurus APJII, Kami Dengan Bangga Mempersembahkan Profil Internet Indonesia 2025," *Asosiasi Penyelenggara Jasa Internet Indonesia*, 2025, <https://survei.apjii.or.id/>.

⁷ Merlyna Lim, "Freedom to Hate: Social Media, Algorithmic Enclaves, and the Rise of Tribal Nationalism in Indonesia," *Critical Asian Studies* 49, no. 3 (July 3, 2017): 411–27, <https://doi.org/10.1080/14672715.2017.1341188>.

manipulasi video untuk pemerasan dan pencemaran nama baik⁸. Fenomena-fenomena ini menunjukkan bahwa kejahatan deepfake di Indonesia tidak terbatas pada satu bentuk tindak pidana, melainkan telah berkembang menjadi instrumen yang digunakan dalam berbagai modus operandi kejahatan yang mengancam keamanan individu maupun kolektif⁹.

Indonesia saat ini berada pada titik kritis dalam merespons ancaman kejahatan deepfake dengan diberlakukannya Kitab Undang-Undang Hukum Pidana (KUHP) baru pada 2 Januari 2026 melalui Undang-Undang Nomor 1 Tahun 2023. Sebelum tahun 2026, kerangka hukum pidana Indonesia yang relevan dengan kejahatan siber terutama diatur oleh KUHP warisan kolonial yang dikodifikasi pada tahun 1918 dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). KUHP lama mengatur beberapa tindak pidana yang dapat diterapkan secara analogi terhadap aspek-aspek tertentu dari kejahatan deepfake, meliputi pemalsuan (Pasal 263), penipuan (Pasal 378), pencemaran nama baik (Pasal 310-321), dan pornografi (Pasal 282). Namun, ketentuan-ketentuan tersebut dirancang untuk kejahatan konvensional dan tidak mengantisipasi kompleksitas teknologi manipulasi digital¹⁰.

Kesenjangan normatif dalam KUHP lama dan UU ITE merupakan landasan utama untuk mengevaluasi kesiapan KUHP baru. Pada KUHP lama, setidaknya terdapat tiga defisiensi normatif utama yang dapat diidentifikasi. Pertama, definisi 'surat' dalam Pasal 263 tentang pemalsuan tidak secara eksplisit mencakup konten multimedia digital seperti video dan audio yang dimanipulasi AI, karena ketentuan tersebut dirumuskan untuk dokumen fisik. Kedua, UU ITE, meskipun lebih modern, tidak secara eksplisit mengatur manipulasi konten menggunakan teknologi AI. Ketentuan-ketentuan tertentu seperti Pasal 27 ayat (3) tentang pencemaran nama baik elektronik dan Pasal 45A tentang penyebaran informasi palsu dapat diterapkan secara terbatas untuk menuntut pelaku deepfake; namun ruang lingkup normatifnya tidak pernah dirancang untuk menangani karakteristik spesifik konten sintetis yang dihasilkan AI¹¹. Ketiga, unsur *mens rea* dalam tindak pidana konvensional tidak mengantisipasi situasi di mana pelaku

⁸ Anisa Rahayu and Kuswandi, "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective," *Indonesian Journal of Law and Justice* 3, no. 2 (December 13, 2025): 14, <https://doi.org/10.47134/ijlj.v3i2.5171>.

⁹ Muhammad Arsalan Khan et al., "Deepfake-Driven Financial Fraud In Indonesia: A Systematic Review Of Economic Impacts And Regulatory Challenges," *INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES* 12, no. 3s (2026): 295–312, <https://doi.org/10.29284/87d1j190>.

¹⁰ Muhammad Ijlal Ramadan and Endik Wahyudi, "Comparative Study: The Urgency Of Reformulating Deepfake Criminal Sanctions In The Criminal Code And The ITE Law Studi Komparatif: Urgensi Reformulasi Sanksi Pidana Deepfake Dalam Kuhp Dan UU ITE," *Jurnal Hukum Sehasen* 11, no. 2 (2025): 353–62.

¹¹ SP SH. MH Sugeng, *Hukum Telematika Indonesia* (Prenada Media, 2020).

memanfaatkan sistem AI yang beroperasi dengan tingkat otonomi tertentu, sehingga menimbulkan pertanyaan mendasar tentang bagaimana niat dapat dibuktikan ketika luaran deepfake dihasilkan oleh algoritma yang mungkin tidak sepenuhnya dipahami atau dikendalikan oleh pelaku. Ketiga kesenjangan normatif ini secara kolektif menciptakan kekosongan hukum yang harus diatasi oleh KUHP baru, dan penelitian ini secara kritis mengevaluasi sejauh mana KUHP baru berhasil melakukannya ¹².

Meskipun literatur internasional tentang regulasi deepfake terus berkembang, masih terdapat kesenjangan signifikan dalam literatur akademik mengenai kesiapan sistem hukum Indonesia dalam menangani kejahatan deepfake. KUHP baru yang baru berlaku pada tahun 2026 belum menjadi subjek analisis akademik mendalam dalam kaitannya dengan kejahatan teknologi kontemporer seperti deepfake, sehingga evaluasi kritis terhadap kesiapannya menjadi sangat mendesak dan relevan.

Permasalahan utama yang dikaji dalam penelitian ini dirumuskan dalam dua pertanyaan penelitian yang saling berkaitan. Pertama, apa karakteristik spesifik kejahatan deepfake di Indonesia ditinjau dari perspektif kriminologi, teknologi, dan viktimologi yang membedakannya dari bentuk-bentuk kejahatan siber lainnya dan mengharuskan adanya respons hukum yang terspesialisasi? Kedua, apakah konstruksi normatif dalam KUHP lama, UU ITE, dan KUHP baru memadai untuk menangani berbagai bentuk dan modus operandi kejahatan deepfake yang teridentifikasi di Indonesia, dan jika terdapat kesenjangan atau kelemahan, bagaimana kesenjangan tersebut harus diatasi?

Penelitian ini diharapkan memberikan kontribusi teoretis dan praktis yang signifikan. Secara teoretis, penelitian ini bertujuan memperkaya diskursus akademik tentang adaptasi hukum pidana terhadap kejahatan berbasis AI generatif di Indonesia. Secara praktis, temuan penelitian diharapkan dapat memberikan masukan konkret bagi para pembuat kebijakan dalam mengevaluasi dan menyempurnakan KUHP baru, memberikan panduan bagi praktisi hukum dalam menafsirkan ketentuan-ketentuannya, serta menyediakan rekomendasi bagi aparat penegak hukum dalam mengembangkan kapasitas forensik digital dan strategi penyelidikan yang efektif.

¹² Rahayu and Kuswandi, "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective."

METODE PENELITIAN

Penelitian ini menggunakan metode normatif yuridis dengan pendekatan doktrinal untuk mengkaji norma-norma hukum positif dalam sistem hukum pidana Indonesia, khususnya ketentuan-ketentuan KUHP lama, KUHP baru, dan UU ITE yang relevan dengan kejahatan deepfake.

Pilihan pendekatan normatif yuridis secara metodologis dibenarkan atas tiga alasan. Pertama, objek utama penelitian ini adalah norma hukum itu sendiri secara khusus, konsistensi internal, kecukupan definitif, dan keterapan ketentuan hukum pidana yang ada terhadap fenomena teknologi baru. Pendekatan doktrinal karenanya tepat karena memungkinkan interpretasi sistematis terhadap teks hukum melalui metode gramatikal, sistematis, historis, dan teleologis tanpa memerlukan pengumpulan data empiris yang mensyaratkan keberadaan yurisprudensi yang sudah berkembang¹³. Kedua, kejahatan deepfake merupakan fenomena yang berkembang dengan pesat, di mana hukum tertulis khususnya KUHP baru yang baru berlaku pada Januari 2026 secara niscaya mendahului akumulasi preseden yudisial. Analisis normatif dengan demikian memberikan kerangka metodologis yang paling tepat untuk mengevaluasi kesiapan hukum dalam ketiadaan yurisprudensi yang sudah berkembang. Ketiga, karena tujuan penelitian adalah mengevaluasi apakah norma hukum yang ada memadai dan merumuskan rekomendasi kebijakan hukum pidana, analisis doktrinal berfungsi sebagai titik awal yang tepat dari mana pengujian empiris dalam praktik peradilan dapat dilakukan selanjutnya¹⁴.

Sumber data terdiri atas bahan hukum primer, meliputi KUHP lama, KUHP baru, dan UU ITE (Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016). Bahan hukum sekunder, mencakup jurnal akademik yang terindeks SINTA dan Scopus, buku teks hukum pidana, dan laporan penelitian tentang teknologi deepfake dan Bahan hukum tersier, meliputi kamus hukum dan ensiklopedia. Pengumpulan data dilakukan melalui kajian pustaka sistematis yang mencakup inventarisasi, identifikasi, dan klasifikasi bahan hukum yang relevan. Data dianalisis secara kualitatif melalui analisis isi dan interpretasi sistematis, yang berlangsung melalui tahapan deskripsi, interpretasi gramatikal sistematis teleologis, evaluasi kecukupan konstruksi normatif, dan perumusan rekomendasi kebijakan hukum pidana.

¹³ Sidi Ahyar Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia," *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (November 30, 2024), <https://doi.org/10.59818/jps.v3i3.1390>.

¹⁴ Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi* (Jakarta: Prenada Media, 2017).

HASIL DAN PEMBAHASAN

Karakteristik Kejahatan Deepfake: Analisis Kriminologis, Teknologis, dan Viktimologis

1. Karakteristik Kriminologis dan Perbedaan dari Kejahatan Siber Lainnya

Kejahatan deepfake di Indonesia memiliki karakteristik unik yang secara fundamental membedakannya dari kejahatan siber konvensional dan membenarkan perlunya pendekatan hukum pidana yang terspesialisasi. Fitur pembeda paling kritis adalah apa yang oleh ¹⁵ disebut sebagai dimensi '*epistemik*' deepfake, berbeda dari kejahatan siber lain yang sekadar menyebarkan informasi palsu, deepfake memproduksi 'bukti yang difabrikasi' yang tampak autentik, sehingga mengikis kepercayaan terhadap semua bentuk bukti digital dan menghasilkan '*liar's dividend*' situasi di mana pelaku dapat menolak bukti yang autentik dengan mengklaim bahwa bukti tersebut adalah deepfake. Erosi epistemik ini secara kategorikal berbeda dari peretasan, phishing, atau penipuan digital konvensional, yang tidak merongrong integritas ontologis bukti digital sebagai sebuah entitas.

Karakteristik pembeda kedua adalah sifat kejahatan hibrida dari deepfake. Dari perspektif kriminologi, deepfake merupakan bentuk kejahatan hibrida yang secara bersamaan menggabungkan unsur-unsur pelanggaran privasi, tindak pidana seksual, penipuan, dan disinformasi dalam satu modus operandi yang dimediasi oleh teknologi AI generatif ¹⁶. Modus operandi yang teridentifikasi di Indonesia meliputi:

1. Pornografi tanpa persetujuan yang melibatkan manipulasi wajah korban ke dalam konten pornografi.
2. Penipuan identitas untuk keuntungan finansial melalui peniruan suara atau wajah tokoh berwenang.
3. Propaganda politik melalui manipulasi pernyataan tokoh publik.
4. Pemerasan dengan melalui ancaman penyebaran konten deepfake yang memalukan ¹⁷.

¹⁵ Chesney and Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security."

¹⁶ Mika Westerlund, "The Emergence of Deepfake Technology: A Review," *Technology Innovation Management Review* 9, no. 11 (2019): 39–52, <https://doi.org/10.22215/TIMREVIEW/1282>.

¹⁷ Muhammad Rizki Kurniarullah et al., "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi" 10, no. 10 (2024): 534–47.

Karakter kejahatan multidimensi ini berarti tidak ada satu pun ketentuan hukum pidana yang ada yang secara memadai menangkap keseluruhan ruang lingkup kerugian yang ditimbulkan, sehingga memerlukan kerangka hukum yang terspesialisasi¹⁸.

Fitur pembeda ketiga berkaitan dengan demokratisasi profil pelaku. Berbeda dari kebanyakan kejahatan siber yang secara historis mensyaratkan keahlian teknis khusus, kejahatan deepfake tidak lagi mengandaikan pelaku yang melek teknologi. Ketersediaan aplikasi pertukaran wajah seperti FaceApp, Reface, dan Zao di toko aplikasi arus utama, serta alat kloning suara seperti Descript dan Resemble.ai, berarti hambatan teknis untuk melakukan tindak pidana ini telah dieliminasi secara efektif¹⁹. Motivasi pelaku di Indonesia sangat beragam dari keuntungan finansial dan balas dendam pribadi hingga kepentingan politik bahkan hiburan tanpa kesadaran akan dampak viktimisasi yang semakin mempersulit pembuktian niat khusus yang disyaratkan oleh ketentuan hukum pidana yang ada. Pola penyebaran konten deepfake mengeksploitasi ekosistem media sosial yang sangat aktif, dengan WhatsApp sebagai platform utama distribusi viral, diikuti oleh Instagram, TikTok, Facebook, dan Twitter²⁰.

2. Karakteristik Teknologis dan Tantangan Deteksi

Dari perspektif teknologi, deepfake dihasilkan menggunakan algoritma pembelajaran mendalam, terutama Generative Adversarial Networks (GAN). GAN terdiri dari dua jaringan neural yang saling bersaing: generator yang memproduksi konten sintetis dan diskriminator yang mengevaluasi keaslian konten. Proses pelatihan iteratif ini menghasilkan konten deepfake dengan tingkat realisme yang semakin tinggi hingga diskriminator tidak lagi dapat membedakan konten sintetis dari material autentik²¹. Teknologi deepfake yang dapat diakses di Indonesia mencakup aplikasi pertukaran wajah, alat kloning suara, aplikasi pornografi deepfake seperti DeepNude, serta perangkat lunak sumber terbuka seperti DeepFaceLab dan FaceSwap yang memberikan kendali lebih terperinci bagi pengguna dengan kemampuan teknis lebih tinggi²².

¹⁸ Siti Nur Azizah and Zaid Alfauza Marpaung, "Criminal Offenses of Misuse of Deepfake Porn Technology Based on Indonesia's Positive Law," *Journal Equity of Law and Governance* 6, no. 1 (2024): 43–49.

¹⁹ Jan Kietzmann et al., "Deepfakes: Trick or Treat?," *Business Horizons* 63, no. 2 (March 2020): 135–46, <https://doi.org/10.1016/j.bushor.2019.11.006>.

²⁰ Lim, "Freedom to Hate: Social Media, Algorithmic Enclaves, and the Rise of Tribal Nationalism in Indonesia."

²¹ Cohen and Giryes, "Generative Adversarial Networks."

²² Westerlund, "The Emergence of Deepfake Technology: A Review."

Tantangan deteksi deepfake di Indonesia cukup besar. Meskipun berbagai metode deteksi berbasis pembelajaran mesin telah dikembangkan menganalisis inkonsistensi dalam gerakan mata, pola kedipan, artefak kompresi, dan ketidaksesuaian pencahayaan metode-metode ini menghadapi perlombaan senjata yang berkelanjutan dengan teknologi pembuatan yang terus berkembang ²³. Kapasitas laboratorium forensik digital Kepolisian Nasional Indonesia dan institusi penegak hukum lainnya untuk mendeteksi dan mengautentikasi konten deepfake masih terbatas, khususnya dalam kasus-kasus yang melibatkan teknologi pembuatan terbaru. Tantangan deteksi ini memiliki implikasi langsung terhadap sistem pembuktian pidana, khususnya menyangkut beban dan standar pembuktian dalam penuntutan perkara deepfake ²⁴.

3. Karakteristik Viktimologis dan Dimensi Kerugian

Dari perspektif viktimologi, kejahatan deepfake menghasilkan bentuk-bentuk viktimisasi yang unik dan menghancurkan yang secara fundamental berbeda dari kejahatan konvensional. ²⁵ mengidentifikasi bahwa viktimisasi digital berbeda dari kejahatan konvensional karena sifatnya yang permanen, dapat direproduksi tanpa batas, dan menyebar secara viral.. Penelitian ²⁶ menunjukkan bahwa korban penyalahgunaan berbasis gambar mengalami tingkat tekanan psikologis yang setara dengan penyintas kekerasan seksual fisik, dengan dimensi tambahan berupa ketidakberdayaan yang muncul dari ketidakmampuan untuk menghentikan penyebaran konten di internet.

Dalam konteks Indonesia, dampak viktimisasi deepfake termanifestasi dalam tiga dimensi yang saling terkait. Dimensi psikologis mencakup trauma, kecemasan, depresi, dan gangguan stres pascatrauma, khususnya bagi korban pornografi deepfake atau pencemaran nama baik berbasis deepfake. Dimensi sosial meliputi stigmatisasi, pengucilan, dan kerusakan reputasi yang permanen; dalam konteks budaya Indonesia yang masih ditandai oleh sikap menyalahkan korban dalam kasus kekerasan seksual,

²³ Ruben Tolosana et al., "Deepfakes and beyond: A Survey of Face Manipulation and Fake Detection," *Information Fusion* 64 (2020): 131–48, <https://doi.org/10.1016/j.inffus.2020.06.014>.

²⁴ Siti Nurkholisah et al., "Tantangan Kriminalisasi Deepfake Dalam Hukum Pidana Indonesia Challenges in Criminalizing Deepfakes under Indonesian Criminal Law," *Jurnal USM Law Review* 8, no. 3 (2025): 1–12.

²⁵ Nicola Henry, Anastasia Powell, and Asher Flynn, "Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse," *A Summary Report*. Melbourne: RMIT University., no. May 2017 (2017): 1–9, file:///C:/Users/AMD-HomeP/AppData/Local/Swiss Academic Software/Citavi 6/ProjectCache/yyrhjpie77pul4jgu8tg75zyyt5j24oeijnccxg1s/Citavi Attachments/b7efbd3f-c6b4-4f14-96c4-bb20a5cd2c50.pdf.

²⁶ Cerens Amanda et al., "Penyalahgunaan Teknologi Deepfake Untuk Konten Pornografi Non-Konsensual Di Indonesia," *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, no. April (2025): 74–81, <https://journal.lpkd.or.id/index.php/Humif/article/view/1475/1961>.

korban pornografi deepfake menghadapi risiko dipersalahkan atas konten yang tidak pernah mereka buat, berujung pada isolasi sosial dan rusaknya hubungan interpersonal. Dimensi ekonomi mencakup kehilangan pekerjaan, kesulitan mendapatkan pekerjaan baru, kerugian finansial terkait upaya penghapusan konten deepfake atau biaya perawatan kesehatan mental, serta pemerasan finansial langsung oleh pelaku yang mengancam penyebaran konten kecuali korban membayar sejumlah uang²⁷.

²⁸ mengidentifikasi tiga dimensi utama yang harus dipertimbangkan dalam membangun kerangka hukum pidana untuk kejahatan berbasis AI, termasuk deepfake. Pertama adalah *actus reus* bagaimana mendefinisikan perbuatan yang dilarang ketika perbuatan tersebut dimediasi oleh algoritma otonom. Kedua adalah *mens rea* bagaimana membuktikan niat atau pengetahuan dalam konteks sistem AI yang kompleks. Ketiga menyangkut pembuktian bagaimana standar pembuktian tradisional dapat beradaptasi dengan realitas di mana bukti digital dapat dimanipulasi secara sempurna menggunakan teknologi deepfake.

Analisis Normatif KUHP Lama dan UU ITE

1. Kesenjangan Normatif dalam KUHP Lama dan UU ITE

KUHP lama yang dikodifikasi pada tahun 1918 tidak secara eksplisit mengatur kejahatan terkait deepfake; namun, beberapa ketentuan dapat diterapkan secara analogi untuk menangani aspek-aspek tertentu dari tindak pidana deepfake, meskipun masing-masing mengungkapkan keterbatasan normatif yang signifikan²⁹.

Pasal 263 tentang Pemalsuan Surat mengatur pembuatan surat palsu dengan niat menggunakannya seolah-olah autentik. Kesenjangan normatif fundamental muncul karena istilah 'surat' dalam doktrin hukum pidana Indonesia secara tradisional dipahami secara sempit sebagai dokumen tertulis fisik³⁰. Video dan audio yang dihasilkan deepfake sulit untuk dikualifikasikan sebagai 'surat' dalam pengertian konvensional ini. Interpretasi gramatikal dan historis menunjukkan bahwa pembuat undang-undang kolonial tidak mengantisipasi keberadaan konten digital yang dapat dimanipulasi

²⁷ Iswandy Rani Saputra et al., "Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber Dan Tantangan Penegakan Hukum Pidana" 12, no. 5 (2025): 255–61.

²⁸ Daniel Schiff et al., "What's Next for AI Ethics, Policy, and Governance? A Global Overview," in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (New York, NY, USA: ACM, 2020), 153–58, <https://doi.org/10.1145/3375627.3375804>.

²⁹ Rahayu and Kuswandi, "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective."

³⁰ Franciscus Theojunior Lamintang, Paulus Anselmus Felix and Lamintang, *Dasar-Dasar Hukum Pidana Di Indonesia* (Sinar Grafika, 2022).

melalui algoritma AI. Meskipun sebagian ahli hukum berpendapat bahwa interpretasi ekstensif dapat diadopsi berdasarkan fungsi pembuktian yang setara, mengandalkan interpretasi analogi dalam hukum pidana berisiko melanggar asas legalitas³¹.

Pasal 378 tentang Penipuan dapat digunakan untuk menuntut pelaku yang menggunakan deepfake sebagai sarana penipuan, misalnya melalui audio deepfake yang meniru suara CEO untuk menginstruksikan transfer dana. Namun, penerapan pasal ini memerlukan pembuktian unsur 'tipu muslihat' dan 'rangkaian kebohongan', yang dalam konteks deepfake menghadirkan tantangan pembuktian teknis khususnya dalam menetapkan bahwa konten tersebut difabrikasi dan sengaja dibuat untuk menipu³². Pasal 310-321 tentang Pencemaran Nama Baik dapat diterapkan pada deepfake yang digunakan untuk merusak reputasi, tetapi konstruksi normatifnya tidak mengantisipasi pencemaran nama baik melalui manipulasi multimedia yang menghasilkan 'bukti visual yang difabrikasi' jauh lebih persuasif daripada pencemaran nama baik verbal atau tekstual konvensional³³. Pasal 282 tentang Kesusilaan dapat diterapkan secara terbatas pada penyebaran pornografi deepfake, namun tidak mengatur pembuatan konten pornografi tanpa persetujuan melalui manipulasi wajah korban, sehingga gagal memberikan perlindungan yang memadai bagi korban³⁴.

Sedangkan dalam UU ITE (Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016), meskipun lebih modern dari KUHP lama, juga menunjukkan kesenjangan normatif yang signifikan dalam menangani kejahatan deepfake. Undang-undang ini tidak secara eksplisit mengatur manipulasi konten berbasis AI. Pasal 27 ayat (3) tentang pencemaran nama baik elektronik dan Pasal 45A tentang penyebaran informasi palsu dapat diterapkan secara terbatas untuk menuntut pelaku deepfake; namun, ruang lingkup normatif ketentuan-ketentuan ini dirancang untuk disinformasi digital konvensional, bukan konten sintesis yang dihasilkan AI³⁵.

Absennya ketentuan dalam UU ITE yang secara spesifik menangani manipulasi biometrik, pembuatan konten sintesis, dan kejahatan yang dimediasi AI merupakan

³¹ Adami Chazawi, *Kejahatan Terhadap Harta Benda* (Media Nusa Creative (MNC Publishing, 2021).

³² Chazawi.

³³ Nurkholisah et al., "Tantangan Kriminalisasi Deepfake Dalam Hukum Pidana Indonesia Challenges in Criminalizing Deepfakes under Indonesian Criminal Law."

³⁴ Annisa Sabilla SH MH Sueni, *DELIK--DELIK DALAM KUHP: KLASIFIKASI, UNSUR DAN ANALISIS YURIDIS (DELIK TERHADAP KEHORMATAN: PENCEMARAN)* (CV. Gita Lentera, 2025).

³⁵ Sugeng, *Hukum Telematika Indonesia*.

kesenjangan normatif kritis. Kerangka pembuktian dan autentikasi dalam undang-undang ini juga mendahului era konten berteknologi AI yang canggih, sehingga standar pembuktiannya tidak secara memadai mengakomodasi situasi di mana konten digital itu sendiri yang lazimnya merupakan bentuk utama bukti tidak dapat dibedakan dari material autentik. Keterbatasan-keterbatasan ini, dikombinasikan dengan keterbatasan KUHP lama, membentuk basis normatif yang dijadikan tolok ukur evaluasi KUHP baru³⁶.

2. Analisis Normatif KUHP Baru dan Kecukupan Konstruksi Normatif

KUHP baru yang berlaku sejak 2 Januari 2026 memuat beberapa ketentuan yang merepresentasikan kemajuan signifikan dalam mengantisipasi kejahatan berbasis teknologi.

Pasal 252-253 tentang Pemalsuan Dokumen Elektronik memperluas konsep pemalsuan melampaui 'surat' untuk mencakup 'dokumen elektronik', yang merupakan kemajuan normatif signifikan yang berpotensi mencakup konten multimedia digital, termasuk video dan audio yang dihasilkan deepfake. Namun, konstruksi normatif ketentuan-ketentuan ini masih harus diuji dalam praktik peradilan untuk menentukan apakah video dan audio deepfake dapat diklasifikasikan sebagai 'dokumen elektronik' dalam pengertian hukum pembuktian suatu hal yang memiliki signifikansi hukum kritis yang diuraikan pada bagian berikut ³⁷.

Pasal 433-434 tentang Penyebaran Informasi yang Menimbulkan Kebencian atau Permusuhan mengatur penyebaran informasi elektronik yang dapat memicu kebencian atau permusuhan. Ketentuan-ketentuan ini dapat diterapkan pada deepfake yang digunakan untuk propaganda politik atau disinformasi yang menghasut. Namun, ketentuan-ketentuan ini dikritik karena berpotensi disalahgunakan untuk menekan kebebasan berekspresi, sehingga memerlukan penerapan yang hati-hati berdasarkan prinsip proporsionalitas ³⁸.

Pasal 418-420 tentang Pelanggaran Privasi melalui Teknologi mengatur pelanggaran privasi melalui teknologi informasi secara lebih komprehensif, termasuk

³⁶ Dimas Kresna Prayoga and Ibrahim Fikma Edrisy, "Urgensi Pengaturan Hukum Terhadap Deepfake Sebagai Alat Kejahatan Siber Dalam Perspektif KUHP Dan UU ITE," *Journal Evidence Of Law* 4, no. 3 (2025): 1666–73, <https://jurnal.erapublikasi.id/index.php/JEL>.

³⁷ Nurkholisah et al., "Tantangan Kriminalisasi Deepfake Dalam Hukum Pidana Indonesia Challenges in Criminalizing Deepfakes under Indonesian Criminal Law."

³⁸ Magdhalena Tasik Todingrara and Heryanto Heryanto, "Penegakan Hukum Terhadap Pelaku Ujaran Kebencian Pada Era 5.0 Berdasarkan Keadilan Pancasila," *Rio Law Jurnal* 6, no. 1 (2024): 73–91, <https://doi.org/10.36355/rlj.v6i1.1617>.

penggunaan data pribadi tanpa persetujuan ketentuan yang relevan untuk kasus deepfake yang melibatkan penggunaan wajah atau suara seseorang secara tidak sah. Namun, konstruksi normatifnya tidak secara eksplisit menyebut manipulasi biometrik sebagai bentuk pelanggaran privasi ³⁹.

Pasal 412-413 tentang Konten Pornografi Tanpa Persetujuan memuat ketentuan yang lebih spesifik yang mengkriminalisasi penyebaran konten pornografi tanpa persetujuan korban, merupakan peningkatan signifikan dibandingkan KUHP lama. Namun, diperlukan klarifikasi lebih lanjut mengenai apakah ketentuan-ketentuan ini mencakup konten pornografi yang dihasilkan melalui manipulasi deepfake, di mana korban sama sekali tidak terlibat dalam pembuatan konten asli apa pun ⁴⁰.

Evaluasi komprehensif terhadap konstruksi normatif KUHP lama dan KUHP baru mengungkapkan ketidakcukupan substansial dalam menangani kejahatan deepfake, meskipun KUHP baru menunjukkan kemajuan yang signifikan. Empat kesenjangan normatif kritis dalam KUHP baru memerlukan telaah mendalam. Kesenjangan pertama dan paling mendasar adalah absennya definisi eksplisit tentang deepfake atau manipulasi konten berbasis AI. Ketiadaan ini menciptakan ketidakpastian hukum mengenai perbuatan spesifik yang dikriminalisasi ⁴¹. Tanpa kejelasan definitif, jaksa penuntut dan pengadilan harus mengandalkan perluasan interpretasi ketentuan yang ada pendekatan yang berisiko melanggar asas legalitas *nullum crimen sine lege*) yang mensyaratkan bahwa perbuatan pidana harus didefinisikan dengan presisi yang cukup untuk memberikan peringatan yang adil kepada calon pelaku dan membatasi penegakan hukum yang sewenang-wenang ⁴². Absennya definisi eksplisit juga menghambat penerapan norma pidana yang konsisten di berbagai forum peradilan, berkontribusi pada fragmentasi hukum.

Kesenjangan kedua berkaitan dengan implikasi hukum dari ambiguitas dalam mengklasifikasikan deepfake sebagai 'dokumen elektronik' dalam sistem pembuktian pidana. Ambiguitas ini bukan sekadar persoalan terminologi, melainkan membawa konsekuensi pembuktian yang mendalam. Jika video dan audio deepfake

³⁹ Arvi Erawan Palindria, Muhammad Sulthan Thufail, and Muhammad Rieval Febrian, "Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia," *Spektrum Hukum* 21, no. 2 (2024): 110, <https://doi.org/10.56444/sh.v21i2.5319>.

⁴⁰ Elang Rinjani Utara and Anis Widyawati, "Analysis of Criminal Law Enforcement on Non-Consensual Deepfake Pornography in the Dissemination of Manipulative Content in Indonesia," *Al-Jinayah : Jurnal Hukum Pidana Islam* 11, no. 1 (June 29, 2025): 125–53, <https://doi.org/10.15642/aj.2025.11.1.125-153>.

⁴¹ Chesney and Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security."

⁴² Chazawi, *Kejahatan Terhadap Harta Benda*.

diklasifikasikan sebagai 'dokumen elektronik' berdasarkan Pasal 252-253 KUHP baru, maka ketentuan pembuktian yang mengatur dokumen elektronik termasuk persyaratan autentikasi, kewajiban rantai penguasaan barang bukti, dan standar penerimaan yang ditetapkan dalam UU ITE akan berlaku secara langsung. Sebaliknya, jika pengadilan memutuskan bahwa konten deepfake tidak memenuhi ambang batas 'dokumen elektronik', jaksa penuntut akan terpaksa mengandalkan ketentuan yang kurang spesifik, sehingga melemahkan basis normatif penuntutan. Lebih jauh, tantangan deteksi deepfake menciptakan paradoks pembuktian yang rekursif: dalam kasus-kasus di mana keaslian konten digital dipersoalkan, fenomena 'liar's dividend' berarti bahwa bahkan bukti yang autentik pun dapat digugat sebagai deepfake, sehingga berpotensi merongrong seluruh kerangka pembuktian suatu penuntutan. Ambiguitas ini mengharuskan adanya klarifikasi legislatif melalui amandemen definitif atau interpretasi yudisial yang mengikat melalui putusan Mahkamah Agung ⁴³.

Kesenjangan ketiga berkaitan dengan perumusan normatif yang tidak jelas mengenai manipulasi biometrik tanpa persetujuan. Meskipun manipulasi wajah dan suara merupakan inti dari kejahatan deepfake, ketentuan-ketentuan KUHP baru tentang pelanggaran privasi (Pasal 418 420) tidak secara eksplisit mengidentifikasi data biometrik sebagai kategori yang dilindungi maupun menetapkan manipulasi biometrik sebagai bentuk perbuatan terlarang yang spesifik. Kelalaian ini cukup signifikan: manipulasi biometrik dalam deepfake berbeda secara kualitatif dari pelanggaran privasi konvensional karena mengambil alih aspek identitas seseorang yang paling intim dan tidak dapat diubah wajah, suara, dan karakteristik biologis untuk tujuan fabrikasi, eksploitasi, atau kerugian ⁴⁴.

Kesenjangan keempat berkaitan dengan konstruksi mens rea dan ketidakcukupannya untuk sistem AI otonom. KUHP baru mempertahankan persyaratan niat konvensional yang tidak mengantisipasi kompleksitas kejahatan yang dimediasi AI. Dalam situasi di mana pelaku memanfaatkan sistem AI yang menghasilkan luaran deepfake melalui proses yang mungkin tidak sepenuhnya mereka pahami atau kendalikan, pembuktian niat khusus yang disyaratkan oleh ketentuan yang ada menjadi

⁴³ Ijzlal Ramadan and Wahyudi, "Comparative Study: The Urgency Of Reformulating Deepfake Criminal Sanctions In The Criminal Code And The ITE Law Studi Komparatif: Urgensi Reformulasi Sanksi Pidana Deepfake Dalam Kuhp Dan UU ITE."

⁴⁴ Palindria, Thufail, and Febrian, "Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia."

bermasalah secara metodologis^{45, 46} berpendapat bahwa penerapan persyaratan mens rea tradisional terhadap kejahatan yang dimediasi AI memerlukan adaptasi doktrinal untuk mengakomodasi kemungkinan constructive knowledge di mana pelaku bertanggung jawab atas luaran sistem AI yang mereka gunakan yang secara wajar dapat diperkirakan daripada mensyaratkan pembuktian pengetahuan aktual atas setiap luaran algoritmik.

Rekomendasi Kebijakan Hukum Pidana

Berdasarkan analisis normatif di atas, rekomendasi kebijakan hukum pidana berikut ini diajukan untuk memastikan kepastian hukum dan perlindungan yang efektif bagi korban kejahatan deepfake di Indonesia.

Pertama, amandemen legislatif paling mendesak adalah pengenalan definisi eksplisit tentang kejahatan deepfake dalam kerangka hukum pidana, dengan menggunakan bahasa yang netral terhadap teknologi namun tepat secara hukum. Definisi tersebut harus mencakup:

1. Manipulasi sintetis yang tidak sah terhadap karakteristik biometrik seseorang termasuk penampilan wajah, suara, dan kemiripan tubuh melalui teknologi AI atau pembelajaran mendalam.
2. Pembuatan, distribusi, atau penguasaan dengan niat mendistribusikan konten sintetis semacam itu tanpa persetujuan yang diberikan secara sadar oleh subjek yang bersangkutan.
3. Tindak pidana yang diperberat di mana konten semacam itu dibuat atau disebarluaskan untuk tujuan eksploitasi seksual, penipuan, pemerasan, atau disinformasi politik.

Perumusan yang netral terhadap teknologi sangat penting untuk memastikan definisi tetap dapat diterapkan seiring perkembangan teknologi deepfake, menghindari keusangan definitif yang melemahkan KUHP lama.

Kedua, ambiguitas pembuktian seputar klasifikasi media deepfake sebagai 'dokumen elektronik' harus diselesaikan melalui amandemen legislatif atau surat edaran Mahkamah Agung yang mengikat. Penyelesaian melalui legislasi lebih diutamakan karena memberikan

⁴⁵ Hendra Prayoga and Hadi Tuasikal, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia," *Abdurrauf Law and Sharia* 2, no. 1 (2025): 22–38, <https://journal.abdurraufinstitute.org/index.php/arlash/article/view/194>.

⁴⁶ Schiff et al., "What's Next for AI Ethics, Policy, and Governance? A Global Overview."

kepastian hukum yang lebih besar dan menghilangkan risiko interpretasi yudisial yang divergen. Amandemen tersebut harus secara eksplisit memasukkan konten audiovisual sintetis yang dihasilkan AI ke dalam ruang lingkup 'dokumen elektronik' untuk keperluan pembuktian pidana, sekaligus menetapkan standar teknis autentikasi termasuk kewajiban analisis forensik oleh institusi forensik digital yang terakreditasi sebelum konten tersebut dapat dijadikan alat bukti dalam persidangan pidana.

Ketiga, penguatan kapasitas kelembagaan dalam bidang forensik digital sangat mendesak. Laboratorium forensik digital Kepolisian Nasional Indonesia dan institusi kejaksaan yang relevan harus dilengkapi dengan teknologi deteksi terkini, diisi oleh spesialis terlatih yang mampu mengautentikasi konten deepfake, dan didukung oleh protokol resmi kerja sama internasional dengan institusi forensik digital asing. Tanpa kapasitas forensik yang sebanding, bahkan ketentuan hukum pidana substantif yang paling baik dirancang sekalipun akan tetap tidak dapat ditegakkan secara praktis.

Keempat, mekanisme perlindungan korban yang komprehensif harus diintegrasikan ke dalam kerangka hukum. Mekanisme ini harus mencakup layanan dukungan psikososial bagi korban deepfake, bantuan hukum yang mudah diakses, mekanisme penghapusan konten yang dapat dipaksakan secara hukum terhadap platform media sosial yang beroperasi di Indonesia, serta skema kompensasi yang mencakup biaya perawatan psikologis, rehabilitasi reputasi, dan kerugian ekonomi. Kerentanan khusus korban perempuan dari pornografi deepfake dalam konteks sosial-budaya Indonesia yang ditandai oleh sikap menyalahkan korban menuntut bahwa ketentuan perlindungan korban dirancang dengan kepekaan eksplisit terhadap kerugian berbasis gender.

Kelima, kampanye literasi digital yang menargetkan profil demografis unik Indonesia yang ditandai oleh literasi digital rendah yang berdampingan dengan penetrasi media sosial yang sangat tinggi sangat penting untuk melengkapi reformasi hukum. Inisiatif pendidikan publik harus menargetkan calon korban maupun calon pelaku, menekankan konsekuensi pidana dari pembuatan dan distribusi deepfake, metode pengenalan dan pelaporan konten deepfake, serta saluran yang tersedia untuk bantuan korban.

KESIMPULAN

Penelitian ini mengidentifikasi dua temuan utama tentang kejahatan deepfake dalam sistem peradilan pidana Indonesia. Pertama, kejahatan deepfake memiliki karakteristik unik yang secara fundamental membedakannya dari kejahatan siber konvensional dan

membenarkan perlunya pendekatan hukum pidana yang terspesialisasi. Dimensi epistemik deepfake kemampuannya memproduksi bukti yang difabrikasi yang tampak autentik dan menghasilkan *'liar's dividend'* membedakannya secara kategorikal dari bentuk-bentuk kejahatan siber lainnya. Sifat kejahatan hibridanya secara bersamaan menggabungkan pelanggaran privasi, tindak pidana seksual, penipuan, dan disinformasi dalam satu modus operandi yang dimediasi AI. Demokratisasi alat pembuatan deepfake telah mengeliminasi hambatan teknis untuk melakukan tindak pidana, memperluas profil pelaku, dan mempersulit pembuktian niat khusus. Secara teknologis, perlombaan senjata antara pembuatan dan deteksi deepfake menciptakan tantangan forensik yang persisten. Secara viktimologis, kejahatan deepfake menyebabkan kerugian psikologis, sosial, dan ekonomi yang menghancurkan yang diperparah oleh konteks budaya Indonesia yang menyalahkan korban serta sifat permanen, dapat direproduksi, dan viral dari konten digital.

Kedua, baik KUHP lama maupun KUHP baru secara tidak memadai menangani kejahatan deepfake, dengan kesenjangan normatif KUHP lama dan UU ITE memberikan basis fundamental untuk mengevaluasi kesiapan KUHP baru. KUHP lama menderita keterbatasan definitif, kesenjangan teknologi, dan ketiadaan regulasi manipulasi biometrik sepenuhnya. Ketentuan-ketentuan UU ITE, meskipun lebih modern, tidak dirancang untuk menangani konten sintesis yang dihasilkan AI dan tidak memiliki kerangka pembuktian serta substantif yang diperlukan untuk penuntutan deepfake yang efektif. KUHP baru menunjukkan kemajuan signifikan dengan memperluas pemalsuan untuk mencakup dokumen elektronik (Pasal 252–253), mengatur pelanggaran privasi digital (Pasal 418–420), dan mengkriminalisasi konten pornografi tanpa persetujuan (Pasal 412–413). Namun, empat kesenjangan kritis masih tersisa: absennya definisi deepfake yang eksplisit yang menciptakan ketidakpastian hukum; ambiguitas dalam mengklasifikasikan media deepfake sebagai 'dokumen elektronik' dengan implikasi pembuktian yang mendalam; perumusan normatif yang tidak jelas mengenai manipulasi biometrik; dan ketidakcukupan konstruksi *mens rea* untuk sistem AI otonom.

Respons kebijakan hukum pidana yang direkomendasikan mencakup: amandemen legislatif eksplisit yang mendefinisikan dan mengkriminalisasi deepfake dengan presisi yang netral terhadap teknologi; penyelesaian ambiguitas klasifikasi dokumen elektronik melalui klarifikasi legislatif atau yudisial; pedoman pembuktian teknis untuk forensik digital dan autentikasi; penguatan kapasitas kelembagaan melalui pelatihan khusus dan kolaborasi pakar internasional; mekanisme perlindungan korban yang komprehensif; dan kampanye literasi digital. Arah penelitian lanjutan yang akan memajukan pengembangan akademik

dan praktis bidang ini meliputi: (a) studi empiris yang mengkaji bagaimana pengadilan Indonesia menerapkan ketentuan KUHP baru pada kasus-kasus deepfake seiring akumulasi preseden yudisial; (b) penelitian sosio-legal tentang efektivitas mekanisme perlindungan korban dalam konteks budaya Indonesia; (c) analisis hukum komparatif terhadap kerangka regulasi deepfake di yurisdiksi civil law yang relevan dengan tradisi hukum Indonesia; dan (d) penelitian interdisipliner teknis-hukum yang mengkaji kecukupan standar forensik digital untuk autentikasi deepfake dalam sistem pembuktian pidana Indonesia. Penelitian-penelitian tersebut akan memberikan landasan empiris yang diperlukan untuk menguji rekomendasi normatif yang diajukan dalam penelitian ini dan untuk secara iteratif menyempurnakan respons hukum pidana Indonesia terhadap kejahatan deepfake.

REFERENSI

- Ajder, Henry, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen. "The State of Deepfakes: Landscape, Threats, and Impact," 2019.
<https://docslib.org/doc/12559428/the-state-of-deepfakes-landscape-threats-and-impact-henry-ajder-giorgio-patrini-francesco-cavalli-and-laurence-cullen-september-2019>.
- Amanda, Cerens, Gea Pitaloka, Fakultas Hukum, Ilmu Sosial, Jurusan Hukum, and Dan Kewarganegaraan. "Penyalahgunaan Teknologi Deepfake Untuk Konten Pornografi Non-Konsensual Di Indonesia." *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, no. April (2025): 74–81.
<https://journal.lpkd.or.id/index.php/Humif/article/view/1475/1961>.
- Amelia, Selvi. "Ruang Cyber vs Kebebasan Berpendapat : Menyeimbangkan Regulasi Dan Ekspresi Di Era Digital Banyak Manfaat Bagi Masyarakat , Terdapat Juga Kekhawatiran Yang Valid." *Staatsrecht Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024).
- APJII. "Survei Penetrasi Internet Dan Perilaku Penggunaan Internet Sebagai Perwakilan Pengurus APJII, Kami Dengan Bangga Mempersembahkan Profil Internet Indonesia 2025." *Asosiasi Penyelenggara Jasa Internet Indonesia*, 2025. <https://survei.apjii.or.id/>.
- Azizah, Siti Nur, and Zaid Alfauza Marpaung. "Criminal Offenses of Misuse of Deepfake Porn Technology Based on Indonesia's Positive Law." *Journal Equity of Law and Governance* 6, no. 1 (2024): 43–49.
- Chazawi, Adami. *Kejahatan Terhadap Harta Benda*. Media Nusa Creative (MNC Publishing, 2021).
- Chesney, Bobby, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>.
- Cohen, Gilad, and Raja Giryes. "Generative Adversarial Networks." In *Machine Learning for Data Science Handbook*, 375–400. Cham: Springer International Publishing, 2023.
https://doi.org/10.1007/978-3-031-24628-9_17.
- Elang Rinjani Utara, and Anis Widyawati. "Analysis of Criminal Law Enforcement on Non-Consensual Deepfake Pornography in the Dissemination of Manipulative Content in

- Indonesia.” *Al-Jinayah : Jurnal Hukum Pidana Islam* 11, no. 1 (June 29, 2025): 125–53. <https://doi.org/10.15642/aj.2025.11.1.125-153>.
- Henry, Nicola, Anastasia Powell, and Asher Flynn. “Not Just ‘Revenge Pornography’: Australians’ Experiences of Image-Based Abuse.” *A Summary Report. Melbourne: RMIT University.*, no. May 2017 (2017): 1–9. file:///C:/Users/AMD-HomeP/AppData/Local/Swiss Academic Software/Citavi 6/ProjectCache/yyrhjpie77pul4jgu8tg75zyyt5j24oeijnccxg1s/Citavi Attachments/b7efbd3f-c6b4-4f14-96c4-bb20a5cd2c50.pdf.
- Ijzlal Ramadan, Muhammad, and Endik Wahyudi. “Comparative Study: The Urgency Of Reformulating Deepfake Criminal Sanctions In The Criminal Code And The ITE Law Studi Komparatif: Urgensi Reformulasi Sanksi Pidana Deepfake Dalam Kuhp Dan UU ITE.” *Jurnal Hukum Sehasen* 11, no. 2 (2025): 353–62.
- Khan, Muhammad Arsalan, Hidayatul Khusnah, Emeraldal Ayu Kusuma, Mar’a Elthaf Ilahiyah, and Muhammad Zeeshan Khan. “Deepfake-Driven Financial Fraud In Indonesia: A Systematic Review Of Economic Impacts And Regulatory Challenges.” *INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES* 12, no. 3s (2026): 295–312. <https://doi.org/10.29284/87d1j190>.
- Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. “Deepfakes: Trick or Treat?” *Business Horizons* 63, no. 2 (March 2020): 135–46. <https://doi.org/10.1016/j.bushor.2019.11.006>.
- Kresna Prayoga, Dimas, and Ibrahim Fikma Edrisy. “Urgensi Pengaturan Hukum Terhadap Deepfake Sebagai Alat Kejahatan Siber Dalam Perspektif KUHP Dan UU ITE.” *Journal Evidence Of Law* 4, no. 3 (2025): 1666–73. <https://jurnal.erapublikasi.id/index.php/JEL>.
- Kurniarullah, Muhammad Rizki, Talitha Nabila, Abdurrahman Khalidy, Vivi Juniarti Tan, and Heni Widiyani. “Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi” 10, no. 10 (2024): 534–47.
- Lamintang, Paulus Anselmus Felix and Lamintang, Franciscus Theojunior. *Dasar-Dasar Hukum Pidana Di Indonesia*. Sinar Grafika, 2022.
- Lim, Merlyna. “Freedom to Hate: Social Media, Algorithmic Enclaves, and the Rise of Tribal Nationalism in Indonesia.” *Critical Asian Studies* 49, no. 3 (July 3, 2017): 411–27. <https://doi.org/10.1080/14672715.2017.1341188>.
- Marzuki, Mahmud. *Penelitian Hukum: Edisi Revisi*. Jakarta: Prenada Media, 2017.
- Nurkholisah, Siti, Daud Rismana, Afrizal Eko Nugroho, Amrina Munjiyah, and Qurota Ayunisa. “Tantangan Kriminalisasi Deepfake Dalam Hukum Pidana Indonesia Challenges in Criminalizing Deepfakes under Indonesian Criminal Law.” *Jurnal USM Law Review* 8, no. 3 (2025): 1–12.
- Palindria, Arvi Erawan, Muhammad Sulthan Thufail, and Muhammad Rieval Febrian. “Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia.” *Spektrum Hukum* 21, no. 2 (2024): 110. <https://doi.org/10.56444/sh.v21i2.5319>.
- Prayoga, Hendra, and Hadi Tuasikal. “Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia.” *Abdurrauf Law and Sharia* 2, no. 1 (2025): 22–38. <https://journal.abdurraufinstitute.org/index.php/arlash/article/view/194>.

- Rahayu, Anisa, and Kuswandi. "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective." *Indonesian Journal of Law and Justice* 3, no. 2 (December 13, 2025): 14. <https://doi.org/10.47134/ijlj.v3i2.5171>.
- Redaksi. "Deepfake Naik 550%, Platform Global Diminta Sediakan Fitur Cek Konten AI - Infodigital.Co.Id." Accessed January 9, 2026. <https://infodigital.co.id/deepfake-naik-550-platform-global-diminta-sediakan-fitur-cek-konten-ai/>.
- Saputra, Iswandy Rani, Rachman Rizal A Sapada, A Dzuqarnain, and Suprpto Suprpto. "Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber Dan Tantangan Penegakan Hukum Pidana" 12, no. 5 (2025): 255–61.
- Schiff, Daniel, Justin Biddle, Jason Borenstein, and Kelly Laas. "What's Next for AI Ethics, Policy, and Governance? A Global Overview." In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 153–58. New York, NY, USA: ACM, 2020. <https://doi.org/10.1145/3375627.3375804>.
- Sueni, Annisa Sabilla SH MH. *DELIK--DELIK DALAM KUHP: KLASIFIKASI, UNSUR DAN ANALISIS YURIDIS (DELIK TERHADAP KEHORMATAN: PENCEMARAN)*. CV. Gita Lentera, 2025.
- Sugeng, SP SH. MH. *Hukum Telematika Indonesia*. Prenada Media, 2020.
- Todingrara, Magdhalena Tasik, and Heryanto Heryanto. "Penegakan Hukum Terhadap Pelaku Ujaran Kebencian Pada Era 5.0 Berdasarkan Keadilan Pancasila." *Rio Law Jurnal* 6, no. 1 (2024): 73–91. <https://doi.org/10.36355/rlj.v6i1.1617>.
- Tolosana, Ruben, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia. "Deepfakes and beyond: A Survey of Face Manipulation and Fake Detection." *Information Fusion* 64 (2020): 131–48. <https://doi.org/10.1016/j.inffus.2020.06.014>.
- Westerlund, Mika. "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review* 9, no. 11 (2019): 39–52. <https://doi.org/10.22215/TIMREVIEW/1282>.
- Wiraguna, Sidi Ahyar. "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia." *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (November 30, 2024). <https://doi.org/10.59818/jps.v3i3.1390>.