

Penerapan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Terhadap Kejahatan *Deepfake* (Studi Putusan Nomor 1295/Pid.Sus/2023/PN Mdn)

Dimas Arvian Muzzaki¹, Lanna Fadilla Citra²

^{1,2}Fakultas Hukum, Universitas Esa Unggul
Dimas.arvian.king@student.esaunggul.ac.id

Abstract

The development of artificial intelligence, particularly deepfake technology, poses serious challenges for Indonesia's legal system by enabling realistic manipulation of visual and audio content, often misused for fraud, defamation, and disinformation. One example is a giveaway scam using a deepfake of actor Baim Wong, causing losses of Rp149 million, decided in Medan District Court Decision Number 1295/Pid.Sus/2023/PN Mdn. This decision reflects legal ambiguity, as enforcement still relies on the Criminal Code and the Electronic Information and Transactions Law through interpretive methods, while Law Number 27 of 2022 on Personal Data Protection (PDP Law) remains underutilized. This research examines the application and effectiveness of the PDP Law against deepfake crimes in the decision, using a normative juridical, descriptive-analytical method with statute, case, and conceptual approaches. Results show the PDP Law was not optimally applied, as the perpetrator was charged only under the ITE Law, while biometric data falsification of face and voice was insufficiently considered. Stronger, consistent application of the PDP Law is needed.

Keywords: artificial intelligence; court decision; cybercrime; deepfake, personal data protection.

Abstrak

Perkembangan teknologi kecerdasan buatan, khususnya deepfake, menciptakan tantangan serius bagi sistem hukum Indonesia karena memungkinkan manipulasi konten visual dan audio secara realistis yang kerap disalahgunakan untuk penipuan, pencemaran nama baik, dan disinformasi. Salah satu contohnya adalah penipuan giveaway menggunakan deepfake artis Baim Wong yang merugikan korban hingga Rp149 juta, sebagaimana diputus dalam Putusan PN Medan Nomor 1295/Pid.Sus/2023/PN Mdn. Putusan ini mencerminkan kekaburan hukum, karena penegak hukum masih mengandalkan KUHP dan UU ITE melalui metode penafsiran, sementara UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) belum dimanfaatkan secara optimal. Penelitian ini mengkaji penerapan dan efektivitas UU PDP terhadap kejahatan deepfake dalam putusan tersebut, menggunakan metode yuridis normatif deskriptif-analitis dengan pendekatan perundang-undangan, kasus, dan konseptual. Hasil menunjukkan UU PDP belum diterapkan secara optimal karena pelaku hanya dijerat UU ITE, sementara unsur pemalsuan data biometrik wajah dan suara belum dipertimbangkan memadai. Diperlukan penguatan penerapan UU PDP secara konsisten.

Kata Kunci: deepfake, kecerdasan buatan, kejahatan siber, perlindungan data pribadi, putusan pengadilan.

Copyright (c) 2026 Dimas Arvian Muzzaki, Lanna Fadilla Citra

✉ Corresponding author: Dimas Arvian Muzzaki

Email Address: Dimas.arvian.king@student.esaunggul.ac.id (Fakultas Hukum, Universitas Esa Unggul)

Received 4 Juli 2025, Accepted 14 Juli 2026, Published 25 Juli 2026

PENDAHULUAN

Semakin berkembangnya teknologi ke era baru yang lebih canggih, menuntut penggunaannya untuk menguasai teknologi dan dapat menyikapi berbagai isu yang berkembang seiring dengan kemajuan teknologi. Khusna dan Pangestuti menyatakan kecanggihan kecerdasan buatan/*artificial intelligence* (AI) memberi banyak kemudahan bagi kehidupan, bahkan sampai bisa mengganti pekerjaan-pekerjaan yang dilakukan oleh manusia (Khusna & Pangestuti, 2019). Salah satu kemajuan yang paling terlihat dalam bidang AI adalah teknologi *deepfake*, yaitu sebuah metode berbasis *deep learning* yang memungkinkan manipulasi konten visual maupun audio dengan tingkat kualitas tinggi sehingga terlihat

seperti asli. Teknologi ini memungkinkan pembuatan video atau audio yang menyerupai seseorang tanpa keterlibatan langsung dari individu yang bersangkutan (Kurniarullah et al., 2024; Prayoga & Tuasikal, 2024).

Floridi menjelaskan bahwa jika dilihat dari sisi positif, teknologi *deepfake* memberikan kontribusi signifikan di berbagai sektor kehidupan. Dalam industri perfilman, teknologi ini memungkinkan restorasi citra wajah aktor yang telah meninggal dunia serta produksi efek visual tingkat tinggi tanpa memerlukan anggaran yang besar. Dalam bidang pendidikan dan kesehatan, *deepfake* dimanfaatkan untuk keperluan simulasi interaktif dan pelatihan tenaga medis melalui pasien virtual. Dalam konteks aksesibilitas, teknologi ini digunakan untuk menghasilkan konten bahasa isyarat secara otomatis bagi penyandang disabilitas tunarungu. Bahkan dalam konteks sejarah, *deepfake* pernah digunakan oleh perusahaan Cere Proc untuk merekonstruksi pidato John F. Kennedy yang tidak sempat disampaikan pada November 1963 (Floridi, 2021). Hal ini sejalan dengan penelitian Khusna dan Pangestuti yang menyatakan bahwa *deepfake* pada hakikatnya merupakan inovasi teknologi yang memungkinkan penyelesaian pekerjaan kompleks secara lebih efisien oleh berbagai kalangan (Khusna & Pangestuti, 2019).

Dalam konteks hukum pidana, Yang menyatakan bahwa teknologi ini telah disalahgunakan untuk kepentingan kejahatan, seperti pornografi non-konsensual, penipuan identitas, pencemaran nama baik, hingga penyebaran disinformasi politik. Fenomena *deepfake* tidak hanya menjadi ancaman terhadap ketertiban umum dan keamanan informasi, tetapi juga menyerang langsung hak-hak fundamental manusia, termasuk hak atas privasi, integritas personal, dan martabat individu. Ketika wajah atau suara seseorang dimanipulasi untuk kepentingan yang melanggar hukum, korban tidak hanya menderita kerugian immaterial tetapi juga kerusakan reputasi yang sulit dipulihkan (Yang, 2025).

Noerman dan Ibrahim menyatakan bahwa hukum sering kali tidak mampu mengikuti laju perubahan yang terjadi dalam masyarakat (Noerman & Ibrahim, 2024). Sejalan dengan hal tersebut, Raharjo melalui teori hukum progresifnya menekankan bahwa hukum seharusnya bersifat fleksibel dan responsif terhadap kebutuhan manusia, serta tidak terjebak dalam kerangka yang kaku di tengah pesatnya perkembangan teknologi (Raharjo, 2019). Dalam konteks kecerdasan buatan, Turner dalam bukunya *Robot Rules: Regulating Artificial Intelligence* menyatakan bahwa pengaturan terhadap AI beserta produk yang dihasilkannya merupakan suatu keharusan, mengingat besarnya dampak yang dapat ditimbulkan oleh teknologi tersebut (Turner, 2019). Selain dari aspek hukum, teknologi pendeteksi *deepfake* juga memegang peranan yang sangat penting, karena kemajuan dalam pembuatan konten palsu terus bersaing dengan upaya pendeteksiannya (Juefei-Xu et al., 2022; Noerman & Ibrahim, 2024).

Kondisi tersebut telah terbukti berkembang luas di Indonesia, termasuk melalui kasus penipuan giveaway yang memanfaatkan rekayasa wajah dan suara artis Baim Wong sehingga menyebabkan kerugian seorang korban bernama Evi yang mencapai Rp149 juta rupiah. Putusan Pengadilan Negeri Medan Nomor 1295/Pid.Sus/2023/PN Mdn merupakan salah satu putusan yang relevan untuk dikaji

secara mendalam. Dalam perkara tersebut, pelaku hanya dijerat Pasal 28 ayat (1) Jo Pasal 45A ayat (1) UU ITE mengenai penyebaran berita bohong dan menyesatkan. Putusan ini mencerminkan realita bahwa aparat penegak hukum mengalami kesulitan menjerat pelaku secara spesifik karena tidak adanya regulasi yang secara eksplisit mengatur kejahatan *deepfake*. Namun, bila dikaji lebih dalam perbuatan pelaku juga melibatkan pemalsuan data biometrik berupa wajah dan suara yang seharusnya dapat dijerat berdasarkan Pasal 65 dan Pasal 66 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) (Noerman & Ibrahim, 2024).

Menurut Arvitto, hingga saat ini Indonesia belum memiliki regulasi yang secara eksplisit mengatur kejahatan *deepfake*. Penegak hukum hanya dapat mengandalkan KUHP, UU ITE, dan UU PDP dengan metode penafsiran hukum, yang menimbulkan kekaburan hukum dan ketidakpastian bagi korban (Arvitto, 2025). Sandoval mengidentifikasi bahwa ancaman terbesar *deepfake* bukan hanya pada individu, tetapi juga terhadap sistem peradilan pidana secara keseluruhan (Sandoval et al., 2024). Oleh karena itu, Basah menyatakan bahwa diperlukan penguatan pada aspek pembuktian dan legislasi yang secara khusus mengatur jenis kejahatan berbasis AI (Basah et al., 2025).

Hapid menegaskan dalam penelitiannya, meskipun Surat Edaran Menkominfo Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial membuka ruang penindakan menggunakan instrumen hukum yang ada, surat edaran tidak memiliki kekuatan hukum mengikat setara undang-undang (Hapid et al., 2024). Oleh karena itu, penelitian ini mengkaji bagaimana penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terhadap kejahatan *deepfake* sebagaimana tercermin dalam Putusan No. 1295/Pid.Sus/2023/PN Mdn, guna memberikan gambaran yang komprehensif mengenai efektivitas regulasi perlindungan data pribadi dalam menjangkau kejahatan *deepfake* di Indonesia.

METODE

Metode yang diterapkan dalam penelitian ini adalah pendekatan hukum yuridis normatif, yang berfokus pada analisis terhadap norma hukum tertulis, prinsip-prinsip hukum, serta keputusan pengadilan yang menjadi objek utama kajian. Pemilihan metode ini didasari tujuan penelitian yang ingin meneliti kecocokan antara tindakan penyalahgunaan teknologi *deepfake* dan ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta penyusunan kebijakan hukum pidana yang optimal untuk menangani kejahatan *deepfake* di Indonesia, terutama yang tergambar dalam Putusan Nomor 1295/Pid.Sus/2023/PN Mdn.

Jenis penelitian yang digunakan adalah deskriptif-analitis, yaitu penelitian yang bertujuan memberikan gambaran secara sistematis, faktual, dan akurat mengenai penyalahgunaan teknologi *deepfake* sebagai pelanggaran data pribadi, serta menganalisis kekaburan regulasi khusus yang mengatur kejahatan tersebut di Indonesia. Penelitian ini menggunakan pendekatan perundang-undangan (*statute approach*) dengan menelaah UU PDP, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP), pendekatan kasus (*case approach*) dengan

menganalisis secara mendalam Putusan Nomor 1295/Pid.Sus/2023/PN Mdn sebagai objek utama penelitian, dan pendekatan konseptual (*conceptual approach*) dengan menggunakan asas legalitas (*nullum crimen nulla poena sine lege*) mengingat terdapat kekaburan hukum (*legal vagueness*) dalam pengaturan kasus kejahatan *deepfake* tersebut.

Sumber data berasal dari data sekunder yang terbagi menjadi tiga kategori. Bahan hukum primer mencakup peraturan perundang-undangan yang relevan serta Putusan Nomor 1295/Pid.Sus/2023/PN Mdn. Bahan hukum sekunder terdiri dari literatur hukum, artikel ilmiah, dan pendapat para ahli yang berkaitan dengan hukum pidana, penggunaan teknologi *deepfake*, perlindungan data pribadi, serta kebijakan hukum pidana. Adapun bahan hukum tersier meliputi kamus hukum dan ensiklopedia (Soekanto & Mamudji, 2001).

Metode pengumpulan data yang diterapkan adalah studi pustaka, meliputi peraturan perundang-undangan, putusan pengadilan, buku ilmiah, dan artikel jurnal yang terkait dengan tindakan kejahatan *deepfake* serta perlindungan data pribadi di Indonesia.

Teknik analisis data yang diterapkan adalah analisis kualitatif, dilakukan dengan menginterpretasikan bahan hukum yang telah dikumpulkan untuk kemudian menjangkau kesimpulan tentang relevansi kejahatan *deepfake* dalam Putusan Nomor 1295/Pid.Sus/2023/PN Mdn dengan ketentuan dalam UU PDP, serta merumuskan kebijakan hukum pidana yang ideal untuk menangani kejahatan *deepfake* di Indonesia.

Teori Hukum Responsif

Teori hukum responsif yang dijelaskan oleh Satjipto Rahardjo menegaskan bahwa hukum tidak bersifat kaku maupun tertutup, tetapi harus sanggup menyesuaikan diri terhadap dinamika sosial yang senantiasa berubah, karena hukum diciptakan untuk manusia, bukan sebaliknya (Rahardjo, 2010).

Noerman dan Ibrahim menyatakan *deepfake* adalah teknologi berbasis Kecerdasan Buatan (AI) yang dapat mengubah wajah, suara, dan video seseorang dengan cara yang sangat realistis sehingga tampak asli, padahal sebenarnya merupakan pemalsuan identitas digital (Noerman & Ibrahim, 2024). Hukum pidana di Indonesia saat ini tidak mampu secara jelas mencakup kejahatan berbasis kecerdasan buatan, sehingga terdapat kekaburan hukum yang berpotensi merugikan masyarakat.

Kekaburan pengaturan yuridis tampak pada Putusan Pengadilan Negeri Medan No. 1295/Pid.Sus/2023/PN Mdn, ketika pelaku hanya dijerat Pasal 28 ayat (1) UU ITE terkait penyampaian informasi palsu, bukan penyalahgunaan identitas digital secara khusus. Berdasarkan teori hukum responsif, situasi tersebut semestinya mendorong pembaruan hukum yang bukan sekadar reaktif, namun antisipatif dalam menyikapi kemajuan teknologi.

Dengan demikian, teori hukum responsif menuntut pemerintah segera merevisi aturan yang berlaku, melalui penambahan substansi dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi ataupun pembentukan regulasi tersendiri terkait pemanfaatan kecerdasan buatan, supaya jaminan hukum bagi korban *deepfake* benar-benar terlaksana dan tidak berhenti pada ranah yuridis normatif.

Teori Negara Hukum (*Rechtsstaat*)

Teori Negara Hukum atau *Rechtsstaat* menekankan bahwa dalam melaksanakan kekuasaan, suatu negara harus tunduk pada hukum, bukan sekadar kekuatan. Kedudukan Indonesia sebagai negara hukum dipertegas melalui Pasal 1 ayat (3) UUD NRI 1945.

Dalam gagasan negara hukum, setiap kejahatan yang menyebabkan kerugian terhadap masyarakat harus memiliki dasar hukum yang jelas sebagai bentuk perlindungan dari negara, sesuai dengan prinsip *nullum crimen nulla poena sine lege*. Sebagaimana dikemukakan Jimly Asshiddiqie, negara hukum modern bukan hanya bertumpu pada kepastian hukum formal, namun juga berhubungan erat dengan jaminan HAM secara fundamental, sehingga negara bertanggung jawab melindungi warganya dari bahaya akibat kemajuan zaman, termasuk kejahatan yang menggunakan teknologi seperti *deepfake*.

Maharani, Rista, dan Luhur menjelaskan bahwa perlindungan data pribadi dalam transaksi digital adalah bagian dari tanggung jawab negara hukum untuk memastikan keamanan hak privasi warganya sebagaimana diatur dalam Pasal 28G ayat (1) UUD NRI 1945 (Maharani, Rista, & Luhur, 2024).

Hubungan konsep negara hukum dengan Putusan Nomor 1295/Pid.Sus/2023/PN Mdn terlihat nyata. Pelaku dikenakan sanksi menurut Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE akibat penyebarluasan berita palsu memakai teknologi *deepfake*. Penerapan pasal tersebut hanya mencakup aspek penyebaran berita palsu dan tidak mengkriminalisasi penyalahgunaan identitas melalui *deepfake* sebagai kejahatan terpisah, sehingga memperlihatkan tidak tepatnya sasaran hukum yang tidak selaras dengan prinsip negara hukum, sebab seluruh perbuatan yang berpotensi merugikan masyarakat semestinya telah memiliki ketentuan yang jelas serta memadai.

Asas Legalitas (*Nullum Crimen Nulla Poena Sine Lege*)

Asas legalitas merupakan pilar fundamental hukum pidana yang tertuang dalam Pasal 1 ayat (1) KUHP, menegaskan bahwa tiada suatu perbuatan dapat dipidana kecuali berdasarkan aturan pidana yang telah ada sebelumnya.

Moeljatno menjelaskan asas legalitas mengandung tiga makna, yaitu larangan analogi, larangan berlaku surut, dan keharusan aturan tertulis (Moeljatno, 2002), yang diperluas oleh Hiariiej menjadi empat prinsip turunan, yakni *lex scripta*, *lex certa*, *lex stricta*, dan *lex praevia* (Hiariiej, 2014). Dalam konteks Putusan Nomor 1295/Pid.Sus/2023/PN Mdn, asas legalitas menghadapi tantangan serius akibat kekaburan hukum (*legal vagueness*) terkait kejahatan *deepfake*. Nurkholisah menyimpulkan bahwa regulasi yang ada belum memenuhi prinsip *lex certa* maupun *lex stricta*, sehingga aparat penegak hukum terpaksa melakukan penafsiran ekstensif yang secara teori bertentangan dengan asas legalitas itu sendiri (Nurkholisah et al., 2025).

Muladi dan Arief menyatakan implikasi yuridis dari kekaburan hukum ini sangat signifikan karena pengaturan yang ada bersifat umum dan belum adaptif terhadap karakteristik manipulasi berbasis teknologi, sehingga korban sulit memperoleh keadilan. Pembentuk undang-undang perlu segera merumuskan norma delik khusus yang secara eksplisit melarang pembuatan, penyimpanan, serta

penyebaran konten sintetis non-konsensual guna memenuhi tuntutan kepastian hukum sekaligus memberikan perlindungan komprehensif bagi masyarakat di era digital (Muladi & Arief, 2005).

Putusan Pengadilan Sebagai Implementasi Hukum

Putusan pengadilan adalah bentuk nyata bagaimana kaidah hukum diaplikasikan dalam kasus konkret, sekaligus indikator utama efektivitas penegakan hukum. Pencermatan terhadap Putusan Nomor 1295/Pid.Sus/2023/PN Mdn menjadi krusial guna mengevaluasi sejauh mana aparat peradilan pidana mampu mengantisipasi kejahatan berbasis kecerdasan buatan, padahal pengaturan teknisnya belum tersedia secara eksplisit.

Nurkholisah menyatakan vakumnya norma hukum yang khusus mengatur kejahatan *deepfake* menyebabkan hakim terpaksa melakukan interpretasi ekstensif terhadap pasal yang sudah ada, sehingga berpotensi memunculkan ambiguitas hukum (Nurkholisah et al., 2025).harus menemukan kekaburan hukum (*rechtsvacuum*).

HASIL DAN PEMBAHASAN

Hasil Penelitian

1. Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terhadap Kejahatan *Deepfake* dalam Putusan No. 1295/Pid.Sus/2023/PN Mdn

Putusan Pengadilan Negeri Medan Nomor 1295/Pid.Sus/2023/PN Mdn merupakan salah satu putusan pertama di Indonesia yang menyidangkan kejahatan dengan modus operandi teknologi *deepfake* berbasis kecerdasan buatan. Terdakwa meretas akun Facebook milik Herlina Efendi menggunakan aplikasi Termux, kemudian membuat postingan palsu mengenai program *giveaway* dari seorang aktor Baim Wong disertai tautan ke akun WhatsApp yang dibuat seolah menjadi akun admin resmi, dengan memanipulasi wajah dan suara Baim Wong melalui teknologi *deepfake*, sehingga korban Evi Afriyanti mengalami kerugian sebesar Rp149.525.000,00. Majelis hakim menjerat terdakwa dengan Pasal 28 ayat (1) Jo Pasal 45A ayat (1) UU ITE dan menjatuhkan pidana penjara selama 4 tahun dan 6 bulan.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mendefinisikan data pribadi sebagai setiap data tentang seseorang baik yang teridentifikasi dan dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya. Berdasarkan Pasal 4 ayat (1) UU PDP, data pribadi terdiri atas dua klasifikasi utama, yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Lebih lanjut, Pasal 4 ayat (2) huruf b UU PDP secara eksplisit mengkategorikan data biometrik sebagai salah satu jenis data pribadi yang bersifat spesifik, bersama dengan data dan informasi kesehatan, data genetika, catatan kejahatan, data anak, dan data keuangan pribadi. Penjelasan Pasal 4 ayat (2) huruf b UU PDP memberikan definisi bahwa yang dimaksud dengan "data biometrik" adalah data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identifikasi unik terhadap individu, seperti gambar wajah. Data biometrik juga menjelaskan sifat keunikan dan/atau karakteristik seseorang yang harus dijaga dan dirawat, termasuk

namun tidak terbatas pada rekam sidik jari, retina mata, dan sampel DNA. Ketentuan ini memiliki relevansi langsung dengan modus operandi kejahatan *deepfake* yang pada intinya mengeksploitasi data biometrik korban khususnya gambar wajah dan karakteristik suara tanpa persetujuan.

Terdapat beberapa pasal dalam UU PDP yang secara langsung dapat diterapkan terhadap perbuatan terdakwa dalam putusan ini. Pertama, Pasal 65 ayat (1) UU PDP melarang setiap orang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian pada subjek data pribadi. Perbuatan terdakwa yang mengambil dan menggunakan data biometrik Baim Wong tanpa izin untuk kepentingan penipuan *giveaway* jelas memenuhi unsur pasal ini.

Kedua, Pasal 66 UU PDP melarang setiap orang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya. Dalam konteks *deepfake*, penyebaran konten sintetis yang menampilkan wajah dan suara korban identitas kepada publik melalui media sosial merupakan bentuk pengungkapan data pribadi yang dilakukan tanpa hak. Ketiga, Pasal 67 ayat (1) dan (2) UU PDP menetapkan sanksi pidana bagi pelanggar, yakni pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5.000.000.000,00 bagi yang memperoleh data pribadi secara melawan hukum, serta pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp4.000.000.000,00 bagi yang mengungkapkan data pribadi tanpa izin.

Apabila ketentuan UU PDP tersebut diterapkan secara kumulatif dengan Pasal 28 ayat (1) UU ITE yang digunakan dalam putusan, maka perlindungan hukum bagi korban akan jauh lebih komprehensif. Pasal 28 ayat (1) UU ITE menjangkau aspek penyebaran informasi palsu yang menimbulkan kerugian konsumen, sementara UU PDP menjangkau aspek penyalahgunaan data biometrik sebagai prasyarat teknis pembuatan konten *deepfake*. Penggabungan penerapan kedua instrumen hukum ini mencerminkan pendekatan yang lebih tepat dalam merespons kejahatan *deepfake* yang bersifat multidimensi.

Menurut Moeljatno, asas legalitas (*nullum crimen nulla poena sine lege*) merupakan fondasi utama hukum pidana modern yang menjamin bahwa seseorang hanya dapat dipidana apabila perbuatannya telah dilarang secara tegas dalam suatu peraturan perundang-undangan yang berlaku sebelum perbuatan tersebut dilakukan. Moeljatno menjelaskan bahwa asas ini mengandung tiga makna pokok, yakni larangan analogi dalam penerapan hukum pidana, larangan berlaku surut (non-retroaktif), dan keharusan aturan tertulis sebagai dasar pemidanaan (Moeljatno, 2002). Hiariej memperluasnya menjadi empat prinsip turunan yang saling melengkapi, yakni *lex scripta* (hukum harus tertulis), *lex certa* (hukum harus jelas dan pasti), *lex stricta* (hukum harus ditafsirkan secara ketat dan tidak boleh dianalogikan), serta *lex praevia* (hukum tidak berlaku surut) (Hiariej, 2014).

Prinsip *lex certa* menghendaki bahwa rumusan delik dalam undang-undang harus cukup jelas, pasti, dan tidak membuka ruang multitafsir yang berlebihan, sehingga setiap orang dapat mengetahui dengan pasti perbuatan apa yang dilarang dan ancaman pidana apa yang menyertainya. Dalam konteks putusan ini, prinsip *lex certa* menghadapi ujian serius karena tidak satupun instrumen hukum yang berlaku di

Indonesia memuat definisi teknis mengenai *deepfake* sebagai modus operandi kejahatan yang berdiri sendiri. UU ITE, UU PDP, maupun KUHP Baru sama-sama tidak secara eksplisit merumuskan *deepfake* sebagai bentuk manipulasi konten digital berbasis kecerdasan buatan.

Nurkholisah menyimpulkan bahwa regulasi yang ada belum memenuhi prinsip *lex certa* maupun *lex stricta* karena tidak memberikan definisi yang cukup jelas mengenai batasan perbuatan yang dilarang dalam konteks manipulasi identitas digital (Nurkholisah et al., 2025). Akibatnya, aparat penegak hukum terpaksa menerapkan Pasal 28 ayat (1) UU ITE yang mengatur penyebaran informasi palsu sebagai pasal terdekat yang dapat menjangkau perbuatan terdakwa. Meskipun penerapan ini secara materiil dapat dibenarkan mengingat adanya unsur penipuan yang jelas, namun secara formal terdapat celah antara rumusan norma yang digunakan dengan karakteristik perbuatan yang sesungguhnya dilakukan terdakwa.

Prinsip *lex stricta* merupakan prinsip yang paling banyak mendapatkan tekanan dalam putusan No. 1295/Pid.Sus/2023/PN Mdn. Prinsip ini melarang hakim untuk melakukan penafsiran yang melampaui makna tekstual rumusan undang-undang (penafsiran ekstensif) apalagi penerapan analogi dalam hukum pidana. Namun dalam praktiknya, ketiadaan norma khusus yang mengatur *deepfake*.

Prinsip *lex praevia* menegaskan bahwa seseorang hanya dapat dipidana berdasarkan hukum yang telah berlaku sebelum perbuatannya dilakukan. Pada dasarnya prinsip *lex scripta* dan *lex praevia* telah terpenuhi dalam putusan No. 1295/Pid.Sus/2023/PN Mdn karena terdakwa dijerat dengan Pasal 28 ayat (1) UU ITE yang memang telah berlaku jauh sebelum perbuatan terdakwa dilakukan. Hal ini menunjukkan bahwa sistem hukum pidana Indonesia berada dalam kondisi ketidakcukupan norma hukum pidana dalam menghadapi kejahatan berbasis kecerdasan buatan, di mana tuntutan keadilan bagi korban dan tuntutan kepastian hukum yang dijamin asas legalitas berhadapan satu sama lain tanpa solusi yang memadai dalam regulasi yang ada. Kondisi ini menegaskan perlunya reformasi legislatif yang tidak hanya mengkriminalisasi *deepfake* secara eksplisit, tetapi juga membangun ekosistem penegakan hukum yang mampu mengikuti perkembangan teknologi secara berkelanjutan termasuk melalui penerapan UU PDP secara lebih optimal sebagaimana diuraikan di atas.

2. Analisis Efektivitas Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terhadap Kejahatan Deepfake (Studi Putusan No. 1295/Pid.Sus/2023/PN Mdn)

Untuk menjawab apakah penerapan UU PDP terhadap kejahatan *deepfake* dapat efektif, penelitian ini menggunakan teori efektivitas hukum sebagaimana dikemukakan oleh Soerjono dan Mamudji, yang mengidentifikasi lima faktor penentu efektivitas hukum, yaitu: (1) substansi hukum; (2) struktur hukum (aparat penegak hukum); (3) budaya hukum; (4) sarana dan prasarana; serta (5) masyarakat (Soerjono & Mamudji, 2015). Kelima faktor ini digunakan sebagai kerangka untuk menilai potensi dan hambatan efektivitas UU PDP, dengan Putusan No. 1295/Pid.Sus/2023/PN Mdn sebagai ilustrasi empirisnya.

Dari aspek substansi hukum, UU PDP memiliki potensi yang cukup untuk dapat efektif, namun mengandung kelemahan struktural dalam menghadapi kejahatan *deepfake*. Pasal 65 UU PDP memang mengatur larangan penggunaan data pribadi orang lain secara tidak sah, namun ketentuan tersebut tidak

secara spesifik menyebut konten sintetis berbasis kecerdasan buatan (AI) sebagai bentuk pelanggaran. Ketiadaan definisi teknis mengenai *deepfake* dalam UU PDP menciptakan celah interpretasi yang berpotensi melemahkan posisi penuntut umum dalam membangun konstruksi dakwaan berbasis undang-undang tersebut, sehingga potensi efektivitasnya baru dapat terealisasi apabila celah ini ditutup.

Dari aspek struktur hukum, Syaputra menyatakan bahwa kapasitas aparat penegak hukum dalam memahami dan menerapkan UU PDP pada kasus-kasus teknologi tinggi seperti *deepfake* masih sangat terbatas. Ketiadaan unit khusus forensik digital yang berpengalaman di sebagian besar institusi kepolisian dan kejaksaan mengakibatkan penanganan kasus *deepfake* dilakukan secara generalis menggunakan instrumen hukum yang paling sering digunakan, yaitu UU ITE, tanpa mempertimbangkan kemungkinan penerapan UU PDP secara kumulatif (Syaputra, 2024).

Untuk menilai lebih jauh apakah penerapan UU PDP terhadap kejahatan *deepfake* dapat efektif, penelitian ini membandingkannya dengan pengaturan *General Data Protection Regulation* (GDPR) di Uni Eropa terhadap kasus-kasus pelanggaran data biometrik. Perbandingan ini menunjukkan bahwa regulasi perlindungan data yang komprehensif mampu memberikan respons hukum yang efektif terhadap penyalahgunaan teknologi AI, termasuk *deepfake*, apabila memenuhi sejumlah syarat. Kunci keberhasilan tersebut terletak pada: (1) ketersediaan definisi teknis yang rinci mengenai data biometrik dan kategori pemrosesan yang dilarang; (2) keberadaan otoritas perlindungan data yang independen dengan kewenangan investigasi dan penegakan hukum yang kuat; serta (3) mekanisme pembuktian yang menempatkan beban pembuktian kepada pengendali data untuk menunjukkan keabsahan pemrosesan.

Indonesia melalui UU PDP telah mengadopsi sebagian elemen-elemen tersebut, sehingga secara normatif UU PDP dapat efektif apabila elemen-elemen yang belum terpenuhi dilengkapi. Noerman dan Ibrahim berpendapat bahwa pembentukan Lembaga Perlindungan Data Pribadi (LPDP) sebagaimana diamanatkan oleh UU PDP merupakan prasyarat fundamental bagi efektivitas penegakan regulasi tersebut. Hingga saat ini, LPDP belum terbentuk secara sempurna, sehingga penegakan UU PDP masih bergantung pada institusi penegak hukum konvensional yang belum memiliki kapasitas teknis yang memadai (Noerman & Ibrahim, 2024). Dengan demikian, dapat dikatakan bahwa UU PDP memiliki potensi efektivitas yang nyata, tetapi potensi tersebut bersifat bersyarat (*conditional*), bergantung pada terpenuhinya prasyarat kelembagaan, teknis, dan operasional yang belum sepenuhnya tersedia saat ini, sebagaimana tergambar dalam Putusan No. 1295/Pid.Sus/2023/PN Mdn.

KESIMPULAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan terhadap Putusan Pengadilan Negeri Medan Nomor 1295/Pid.Sus/2023/PN Mdn dalam kaitannya dengan penerapan UU PDP, formulasi kebijakan hukum pidana yang ideal, dan analisis asas legalitas, maka dapat ditarik kesimpulan sebagai berikut.

Pertama, penerapan UU PDP terhadap kejahatan *deepfake* dalam Putusan No. 1295/Pid.Sus/2023/PN Mdn belum optimal. Majelis hakim hanya menjerat terdakwa dengan Pasal 28 ayat (1) UU ITE tanpa mengikutsertakan UU PDP, sedangkan perbuatan memanipulasi wajah dan suara korban tanpa persetujuan sebenarnya telah memenuhi unsur pemrosesan data biometrik secara melawan hukum dalam Pasal 65 ayat (1), Pasal 66, dan Pasal 67 UU PDP. Hal ini terjadi bukan karena norma UU PDP tidak mampu menjangkau perbuatan terdakwa, melainkan karena aparat penegak hukum belum menggunakan penafsiran yang lebih luas terhadap ketentuan yang sebenarnya berlaku bagi setiap pihak yang memproses data biometrik tanpa dasar hukum yang sah. Di sisi lain, ketergantungan hakim pada UU ITE memunculkan ketegangan dengan asas legalitas, khususnya prinsip *lex certa* dan *lex stricta*, sebab Pasal 28 ayat (1) UU ITE tidak memuat definisi *deepfake* sehingga penerapannya menuntut penafsiran yang melampaui makna tekstual pasal. Meskipun prinsip *lex scripta* dan *lex praevia* masih terpenuhi, ketegangan ini menunjukkan bahwa hukum pidana Indonesia belum siap menghadapi kejahatan *deepfake*. Karena itu, penerapan UU PDP secara integratif bersama UU ITE dengan dukungan penafsiran hukum yang progresif perlu ditempuh agar perlindungan bagi korban *deepfake* lebih komprehensif, sekaligus mendorong reformasi legislatif yang secara tegas mengkriminalisasi *deepfake* ke depan.

Kedua, berdasarkan hasil penelitian tersebut, dapat disimpulkan bahwa penerapan UU PDP terhadap kejahatan *deepfake* belum efektif dalam praktik peradilan saat ini, namun secara normatif tetap berpotensi dapat efektif apabila sejumlah prasyarat dipenuhi, sebab ketidakefektifan yang terjadi lebih disebabkan oleh faktor implementasi, bukan oleh ketiadaan landasan hukum dalam UU PDP itu sendiri. Agar potensi efektivitas tersebut dapat terwujud, diperlukan empat langkah utama, yaitu penerbitan peraturan pelaksana yang memuat definisi teknis mengenai *deepfake* dan pemrosesan data biometrik berbasis AI, penguatan kapasitas kelembagaan aparat penegak hukum termasuk unit forensik digital, percepatan pembentukan LPDP dengan kewenangan investigasi dan penegakan yang memadai, serta penerapan UU PDP secara kumulatif bersama UU ITE dalam penanganan perkara *deepfake* ke depan.

DAFTAR PUSTAKA

Undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) jo. UU No. 19/2016 jo. UU No. 1/2024.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang Undang Hukum Pidana (KUHP).

Putusan No. 1295/Pid.Sus/2023/PN Mdn.

Arvitto, R. S. (2025). Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia*, 4(2), 73–82. <https://doi.org/10.35912/jihham.v4i2.3937>

Basah, D. A. Y., Wijaya, A., & Januardy, I. (2025). Kriminalisasi Pelanggaran Protokol Digital. 5, 386–398.

- Floridi, L. (2021). Artificial Intelligence, Deepfakes and a Future of Ectypes. *Philosophical Studies Series*, 144(Springer, Charm).
- Hapid, F. M., Suntana, I., & Royani, M. Y. (2024). Rujukan rumas 3. *Jurnal USM Law Review*, 7(3), 1155–1174.
- Hiariej, E. O. S. (2014). *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka.
- Juefei-Xu, F., Run, W., Huang, Y., Guo, Q., Ma, L., & Liu, Y. (2022). Countering Malicious DeepFakes: Survey, Battleground, and Horizon. *International Journal of Computer Vision*, 130, 1678–1734.
- Khusna, I. H., & Pangestuti, S. (2019). Deepfake, Tantangan Baru Untuk Netizen. *Agustus 1945 Jakarta 1 Promedia*, 5(2), 1–24.
- Kurniarullah, M. R., Nabila, T., Khalidy, A., Tan, V. J., & Widiyani, H. (2024). Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: DeepfakePornografi dan Pencurian Data Pribadi. 10(10), 534–547.
- Maharani; Rista, & Luhur, P. A. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection of Consumer Personal Data by Electronic System Providers in Digital Peningkatan substansial dalam penggunaan platform e-commerce di Indonesia telah. *Jurnal Usm Law Review*, 7(1), 333–347.
- Marzuki, P. M. (2021). *Penelitian hukum (Edisi revisi)*. Prenada Media.
- Moeljatno. (2002). *Asas-Asas Hukum Pidana (Edisi Revisi)*. Jakarta: Rineka Cipta.
- Muladi, & Arief, B. N. (2005). *Teori-Teori dan Kebijakan Pidana*. Bandung: Alumni.
- Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Perlindungan Negara. *Jurnal USM LAW REVIEW*, 7 No. 2(2), 1–4.<https://journals.usm.ac.id/index.php/julr/article/download/8995/4174/28119>
- Nurkholisah, S., Risma, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Tantangan Kriminalisasi Deepfake dalam Hukum Pidana Indonesia Challenges in Criminalizing Deepfakes under Indonesian Criminal Law. *Jurnal Usm Law Review*, 8(3), 1–12. <https://journals.usm.ac.id/index.php/julr/article/view/13060>
- Prayoga, H., & Tuasikal, H. (2024). Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia. 1(2), 22–38.
- Rahardjo, S. (2010). *Penegakan Hukum Progresif*. PT Kompas Media Nusantara.
- Raharjo, B. (2019). Teori Etika Dalam Kecerdasan Buatan (AI). In Yayasan Prima Agus Teknik.
- Sandoval, M. P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review. *Crime Science*, 13(1), 1–16. <https://doi.org/10.1186/s40163-024-00239-1>
- Soekanto, S., & Mamudji, S. (2001). *Normative legal research: A brief overview*. Raja Grafindo Persada.
- Soerjono, S., & Mamudji, S. (2015). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. PT Raja Grafindo Persada.

- Syaputra, R. (2024). Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence(AI) dari Perspektif Hukum Pidana Indonesia. Jurnal Hukum Respublica, Fakultas Hukum Universitas Lancang Kuning, 5–12.
- Turner, J. (2019). Robot Rules: Regulating Artificial Intelligence. Springer International Publishing.
- Yang, M. (2025). Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.1. No.4 (Juli 2020) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) <https://jhlrg.rewangrencang.com/>. Rewang Rencang : Jurnal Hukum Lex Generalis, 6(7), 1–13.