



**PENEGAKAN HUKUM TERHADAP PENYALAHGUNAAN ARTIFICIAL
INTELLIGENCE MELALUI TEKNOLOGI DEEPPAKE DALAM TINDAK
PIDANA SIBER
(Studi pada Direktorat Reserse Siber Polda Sumatera Utara)**

Mulia Akbar Batubara¹, Azmiati Zuliah², Andi Maysarah³

Mahasiwa Fakultas Hukum Universitas Dharmawangsa¹

Dosen Fakultas Hukum Universitas Dharmawangsa²

Dosen Fakultas Hukum Universitas Dharmawangsa³

Email : muliaakbarbatubara@gmail.com

ABSTRAK

Perkembangan Artificial Intelligence (AI) memberikan kontribusi besar bagi kemajuan teknologi, namun di sisi lain membuka peluang terjadinya penyalahgunaan melalui teknologi deepfake. Teknologi ini dapat memanipulasi wajah, suara, maupun video sehingga tampak menyerupai aslinya dan berpotensi dimanfaatkan untuk penipuan, pemerasan, pencemaran nama baik, penyebaran hoaks, serta berbagai bentuk tindak pidana siber lainnya. Penelitian ini bertujuan untuk mengkaji pengaturan hukum di Indonesia terkait penyalahgunaan AI melalui deepfake, pelaksanaan penegakan hukum oleh Direktorat Reserse Siber Polda Sumatera Utara, dan hambatan yang dihadapi dalam proses penanganannya. Metode yang digunakan adalah penelitian hukum empiris dengan pendekatan perundang-undangan dan pendekatan kasus. Data diperoleh melalui studi literatur dan wawancara dengan aparat penegak hukum. Hasil penelitian menunjukkan bahwa pengaturan mengenai deepfake masih tersebar dalam berbagai peraturan, terutama UU ITE dan KUHP, sehingga belum membentuk kerangka hukum yang komprehensif. Penegakan hukum dilakukan melalui penyelidikan digital, analisis forensik elektronik, pelacakan akun, dan kerja sama dengan penyelenggara sistem elektronik.

Kata Kunci : *Artificial Intelligence, deepfake, tindak pidana siber, penegakan hukum, forensik digital.*

ABSTRACT

The advancement of Artificial Intelligence (AI) has contributed significantly to technological innovation, yet it has also created opportunities for misuse through deepfake technology. This technology is capable of manipulating facial images, voices, and videos so that they appear authentic, and may be used for fraud, extortion, defamation, the dissemination of false information, and various forms of cybercrime. This study aims to examine the legal framework in Indonesia regarding the misuse of AI through deepfake technology, the law enforcement practices carried out by the Cyber Crime Directorate of the North Sumatra Regional Police, and the obstacles encountered in handling such cases. The research employs an empirical legal method using statutory and case approaches. Data were



collected through literature review and interviews with law enforcement officers. The

findings indicate that regulations concerning deepfake misuse are still dispersed across several legal instruments, particularly the Electronic Information and Transactions Law and the Criminal Code, and therefore have not yet established a comprehensive legal framework for AI-based crimes. Law enforcement is conducted through digital investigations, electronic forensic analysis, account tracing, and cooperation with electronic system providers. The main challenges include the absence of specific regulations, difficulties in digital forensic evidence, limited human resources, and the transnational nature of cybercrime.

Keywords: Artificial Intelligence, deepfake, cybercrime, law enforcement, digital forensics.

1. PENDAHULUAN

Perkembangan teknologi digital yang berlangsung sangat cepat telah mendorong pemanfaatan *Artificial Intelligence* (AI) dalam berbagai aspek kehidupan, mulai dari komunikasi, aktivitas ekonomi, hingga sistem penegakan hukum. AI tidak lagi diposisikan sekadar sebagai perangkat otomatisasi, melainkan telah berevolusi menjadi teknologi yang mampu menghasilkan konten visual, audio, dan video secara mandiri melalui mekanisme generative AI. Salah satu inovasi yang paling menonjol adalah teknologi deepfake, yaitu teknik manipulasi digital berbasis machine learning dan deep neural networks yang dapat menghasilkan gambar, suara, atau video yang tampak nyata meskipun merupakan rekayasa komputer.¹

Dari perspektif doktrin hukum pidana digital (*digital criminal law*), ruang siber dipandang sebagai wilayah hukum yang memiliki karakteristik khusus karena tindak pidana dapat dilakukan secara anonim, melintasi batas negara, dan mengandalkan alat bukti elektronik sebagai sarana pembuktian utama. Dalam praktik deepfake, objek yang direkayasa bukan lagi benda fisik, melainkan representasi digital berupa citra, suara, dan data elektronik. Oleh karena itu, pertanggungjawaban pidana tidak hanya didasarkan pada akibat yang ditimbulkan, tetapi juga pada kesengajaan pelaku dalam menggunakan teknologi AI untuk menipu, merugikan, atau menyerang kehormatan pihak lain.²

¹ Ahmad Rizki, "Pertanggungjawaban Pidana terhadap Manipulasi Konten Digital Berbasis Artificial Intelligence," *Jurnal Hukum IUS QUIA IUSTUM* 31, no. 2 (2024): 215–230

² Muhammad Fadli, "Deepfake sebagai Ancaman Baru dalam Sistem Hukum Pidana Digital," *Jurnal Legislasi*



Pada mulanya, teknologi *deepfake* dikembangkan untuk kepentingan hiburan, pendidikan, dan industri kreatif. Namun, seiring dengan meningkatnya akses terhadap

teknologi AI, penggunaannya mulai bergeser ke arah yang melanggar hukum, seperti penipuan daring, pemerasan, pencemaran nama baik, penyebaran konten pornografi tanpa persetujuan, pencurian identitas digital, serta penyebaran disinformasi politik. Kondisi ini menimbulkan ancaman serius terhadap keamanan siber, perlindungan data pribadi, dan kepastian hukum karena masyarakat semakin sulit membedakan antara konten asli dan konten hasil manipulasi AI.³

Dalam kajian teori hukum pidana, penyalahgunaan *deepfake* dapat dianalisis melalui beberapa pendekatan. Teori absolut (retributif) memandang pidana sebagai bentuk pembalasan atas perbuatan melawan hukum yang dilakukan pelaku. Sementara itu, teori relatif (tujuan) *menempatkan* pidana sebagai instrumen pencegahan, baik untuk mencegah pelaku mengulangi perbuatannya maupun memberikan efek jera kepada masyarakat. Adapun teori gabungan mengintegrasikan unsur pembalasan dan pencegahan sehingga dianggap paling relevan untuk diterapkan terhadap tindak pidana berbasis AI karena selain menghukum pelaku, juga bertujuan melindungi masyarakat dan menjaga kepercayaan publik terhadap ekosistem digital.⁴

Di Indonesia, pengaturan mengenai tindak pidana siber tersebar dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Meskipun ketiga regulasi tersebut dapat digunakan untuk menindak pelaku, hingga saat ini belum terdapat ketentuan yang secara spesifik mengatur penyalahgunaan AI melalui teknologi *deepfake*. Akibatnya, penegakan hukum masih bergantung pada penafsiran terhadap pasal-pasal umum yang belum

Indonesia 21, no. 4 (2024): 511–528.

³ Dewi Kartika Sari, "Perlindungan Hukum terhadap Korban Deepfake dalam Perspektif UU ITE," Jurnal RechtsVinding 13, no. 3 (2024): 401–418.

⁴ Sri Wahyuni, "Analisis Teori Pemidanaan terhadap Tindak Pidana Siber," Jurnal Hukum dan Peradilan 13, no. 1 (2024): 97–114.

sepenuhnya mampu menjawab karakteristik kejahatan berbasis AI.⁵

Secara nasional, kecenderungan penyalahgunaan deepfake terus mengalami peningkatan. PT Indonesia Digital Identity (VIDA) mencatat bahwa kasus penipuan yang memanfaatkan teknologi *deepfake* meningkat sekitar 1.550% pada periode 2022–2023. Selain itu, laporan Sensity AI menunjukkan bahwa jumlah konten deepfake di tingkat global bertambah sekitar 550% dalam lima tahun terakhir seiring dengan semakin mudahnya akses terhadap teknologi generative AI.⁶

Di Sumatera Utara, peningkatan penyalahgunaan AI berbasis deepfake dapat dilihat dari tren laporan yang diterima Direktorat Reserse Siber Polda Sumatera Utara sebagaimana tabel berikut.

Tabel 1.
Tren Laporan Dugaan Penyalahgunaan AI Deepfake di Sumatera Utara
2022–Semester I 2025

Tahun	Jumlah Kasus/Laporan	Bentuk Penyalahgunaan
2022	3 kasus	Manipulasi foto dan video untuk penipuan daring serta pencemaran nama baik.
2023	8 kasus	Pemalsuan identitas digital dan penipuan berbasis media sosial.
2024	15 kasus	Video manipulatif bermuatan politik, pemerasan, dan penyebaran konten palsu.
2025 (s.d. Semester I)	22 laporan	Manipulasi suara dan video berbasis AI untuk penipuan, pemerasan, dan disinformasi.

Sumber: Hasil wawancara penelitian dengan Direktorat Reserse Siber Polda Sumatera Utara dan data penanganan perkara tahun 2022–2025.

Tabel tersebut menunjukkan adanya peningkatan yang cukup tajam dari tahun ke tahun. Kenaikan jumlah laporan tidak hanya mencerminkan semakin luasnya penggunaan

⁵ Fauzan Nasution, "Kebijakan Hukum Pidana terhadap Kejahatan Siber Berbasis Artificial Intelligence," Jurnal Penelitian Hukum De Jure 24, no. 2 (2024): 189–204.

⁶ Yuniarti, "Efektivitas Penegakan Hukum terhadap Kejahatan Siber di Indonesia," Jurnal Mimbar Hukum 36, no. 2 (2024): 267–283.



teknologi deepfake, tetapi juga menunjukkan bahwa ancaman kejahatan berbasis AI telah menjadi persoalan nyata dalam sistem penegakan hukum daerah. Peningkatan kasus ini memperkuat argumentasi bahwa hukum pidana konvensional menghadapi tantangan baru akibat munculnya bentuk kejahatan yang berbasis algoritma dan data digital.

Menurut teori penegakan hukum yang dikembangkan oleh Soerjono Soekanto, keberhasilan penegakan hukum dipengaruhi oleh lima unsur utama, yaitu substansi hukum, aparat penegak hukum, sarana atau fasilitas pendukung, masyarakat, dan budaya hukum.⁷ Dalam konteks penanganan tindak pidana deepfake, aspek substansi hukum tercermin dari belum tersedianya regulasi yang secara khusus mengatur penyalahgunaan AI dan teknologi deepfake. Dari sisi aparat penegak hukum, masih terdapat keterbatasan jumlah penyidik yang memiliki kompetensi di bidang forensik AI dan analisis digital. Sementara itu, faktor sarana dan prasarana berkaitan dengan kebutuhan laboratorium forensik digital yang lebih modern dan mampu mendeteksi manipulasi berbasis AI. Pada faktor masyarakat, rendahnya literasi digital menyebabkan banyak pengguna internet belum mampu membedakan konten asli dengan konten hasil rekayasa. Adapun faktor budaya hukum terlihat dari kecenderungan sebagian masyarakat untuk menyebarkan informasi tanpa melakukan verifikasi terlebih dahulu.

Penegakan hukum terhadap penyalahgunaan *deepfake* juga memerlukan pendekatan yang berbeda dengan tindak pidana konvensional karena karakter kejahatan siber bersifat borderless. Pelaku dapat memanfaatkan server yang berada di luar negeri, menggunakan identitas anonim, serta mengoperasikan platform digital yang berada di luar yurisdiksi nasional. Oleh karena itu, proses pembuktian tidak cukup hanya mengandalkan alat bukti konvensional, tetapi harus didukung oleh forensik digital yang mampu menelusuri metadata, pola piksel, audio fingerprint, dan jejak algoritmik dari proses generatif AI.⁸ Kompleksitas tersebut menjadikan penanganan perkara deepfake jauh lebih rumit dibandingkan dengan tindak pidana siber konvensional.

⁷ Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum* (Jakarta: RajaGrafindo Persada, 2019), hlm. 8–10.

⁸ Widodo, *Hukum Pidana di Bidang Teknologi Informasi Cybercrime Law* (Yogyakarta: Aswaja Pressindo, 2013), hlm. 112–118.

Direktorat Reserse Siber Polda Sumatera Utara memiliki posisi strategis dalam melakukan penyelidikan, penyidikan, dan pembuktian terhadap tindak pidana yang memanfaatkan teknologi AI. Akan tetapi, peningkatan jumlah laporan dugaan penyalahgunaan deepfake menunjukkan bahwa kapasitas penegakan hukum perlu terus diperkuat, baik melalui peningkatan kompetensi sumber daya manusia, pengembangan teknologi forensik digital, maupun penguatan kerja sama dengan berbagai pihak terkait agar mampu mengimbangi perkembangan teknologi yang berlangsung sangat cepat.

Berdasarkan kondisi tersebut, penelitian ini penting dilakukan untuk mengkaji secara mendalam pengaturan hukum mengenai penyalahgunaan AI melalui teknologi *deepfake*, implementasi penegakan hukum pada Direktorat Reserse Siber Polda Sumatera Utara, serta berbagai hambatan yang dihadapi dalam penanganan tindak pidana siber berbasis AI. Hasil penelitian diharapkan dapat memberikan sumbangan teoritis bagi pengembangan doktrin hukum pidana digital sekaligus menjadi masukan praktis dalam perumusan kebijakan penegakan hukum terhadap penyalahgunaan teknologi *deepfake* di Indonesia.

2. METODE PENELITIAN

Penelitian ini menerapkan metode penelitian hukum empiris⁹ dengan menggunakan dua pendekatan, yaitu pendekatan perundang-undangan (*statute approach*) dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai ketentuan hukum yang mengatur tindak pidana siber berbasis Artificial Intelligence, terutama yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, dan Kitab Undang-Undang Hukum Pidana.

Bahan penelitian terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara langsung dengan aparat penegak hukum pada Direktorat Reserse Siber Polda Sumatera Utara yang menangani perkara terkait kejahatan siber. Adapun data sekunder dikumpulkan melalui studi kepustakaan terhadap peraturan perundang-undangan, buku-buku hukum, artikel jurnal ilmiah, serta dokumen lain yang relevan

⁹ Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2021), hlm. 133–136.



dengan pokok permasalahan penelitian.¹⁰

Seluruh data yang terkumpul dianalisis secara kualitatif dengan menghubungkan fakta-fakta yang ditemukan di lapangan dengan teori hukum dan ketentuan normatif yang berlaku. Melalui analisis tersebut diharapkan diperoleh gambaran yang menyeluruh mengenai pengaturan hukum, praktik penegakan hukum, serta hambatan yang dihadapi dalam penanganan penyalahgunaan teknologi *deepfake* berbasis AI.¹¹

3. HASIL PENELITIAN DAN PEMBAHASAN

Pengaturan Hukum Penyalahgunaan Artificial Intelligence melalui Teknologi *Deepfake*

Pengaturan hukum mengenai penyalahgunaan Artificial Intelligence (AI) melalui teknologi *deepfake* di Indonesia hingga saat ini belum dituangkan dalam satu regulasi khusus yang bersifat komprehensif. Kondisi tersebut menunjukkan bahwa perkembangan teknologi kecerdasan buatan berlangsung lebih cepat dibandingkan pembentukan perangkat hukum yang mengaturnya. Akibatnya, aparat penegak hukum masih harus mendasarkan penindakan pada berbagai ketentuan yang tersebar dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pelindungan Data Pribadi (UU PDP), Kitab Undang-Undang Hukum Pidana (KUHP), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Privat.¹²

Dalam perspektif teori negara hukum, negara mempunyai kewajiban untuk memberikan perlindungan terhadap hak-hak warga negara melalui pembentukan regulasi yang mampu menyesuaikan diri dengan perkembangan teknologi. Konsep negara hukum Pancasila menempatkan hukum sebagai sarana untuk melindungi martabat manusia dan

¹⁰ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: RajaGrafindo Persada, 2018), hlm. 12–15.

¹¹ Amiruddin dan Zainal Asikin, *Pengantar Metode Penelitian Hukum* (Jakarta: RajaGrafindo Persada, 2019), hlm. 167–170.

¹² Widodo, *Hukum Pidana di Bidang Teknologi Informasi Cybercrime Law* (Yogyakarta: Aswaja Pressindo, 2013), hlm. 112–118.



mewujudkan keadilan sosial.¹³ Oleh karena itu, penyalahgunaan deepfake yang menyerang identitas, reputasi, dan privasi seseorang harus dipahami sebagai ancaman terhadap hak konstitusional warga negara. Dari sudut pandang hak asasi manusia, penggunaan wajah, suara, atau video seseorang tanpa persetujuan untuk kepentingan pembuatan deepfake berpotensi melanggar hak atas privasi dan perlindungan diri sebagaimana dijamin dalam Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.¹⁴ Kerugian yang ditimbulkan tidak hanya bersifat ekonomi, tetapi juga dapat merusak kehormatan dan martabat individu.

UU ITE merupakan regulasi yang paling sering digunakan dalam penanganan perkara *deepfake*. Pasal 27 dapat diterapkan terhadap distribusi konten yang melanggar kesusilaan atau mencemarkan nama baik, Pasal 28 terhadap penyebaran informasi bohong yang menimbulkan kerugian, sedangkan Pasal 35 mengatur manipulasi informasi elektronik sehingga tampak seolah-olah autentik.¹⁵ Dalam perkara deepfake, Pasal 35 menjadi sangat relevan karena teknologi tersebut pada dasarnya memanipulasi informasi elektronik berupa gambar, suara, atau video.

Aspek yang sangat penting dalam penegakan hukum terhadap deepfake adalah Pasal 5 UU ITE yang mengakui informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya sebagai alat bukti hukum yang sah.¹⁶ Ketentuan ini memberikan dasar yuridis bagi penggunaan rekaman digital, metadata, hasil analisis forensik, dan jejak algoritma AI sebagai alat bukti dalam proses peradilan pidana. Tanpa pengakuan terhadap alat bukti elektronik, pembuktian tindak pidana deepfake akan menghadapi kesulitan karena objek kejahatan berada dalam bentuk digital. Dalam praktik forensik digital, penyidik dapat menganalisis metadata, pola piksel gambar, audio fingerprint, serta jejak proses generatif AI untuk membuktikan adanya manipulasi digital.

¹³ Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia* (Surabaya: Bina Ilmu, 1987), hlm. 25–27.

¹⁴ Jimly Asshiddiqie, *Konstitusi dan Konstitusionalisme Indonesia* (Jakarta: Sinar Grafika, 2010), hlm. 181–184.

¹⁵ Lihat Ketentuan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

¹⁶ Rudi Hartono, "Pembuktian Forensik Digital pada Tindak Pidana Siber," *Jurnal Yudisial* 17, no. 1 (2024): 55–72.

UU PDP juga mempunyai peranan penting karena banyak praktik deepfake menggunakan foto, video, atau rekaman suara seseorang yang diambil dari media sosial tanpa persetujuan yang sah.¹⁷ Tindakan tersebut berpotensi melanggar prinsip pemrosesan data pribadi yang sah, terbatas, dan transparan sebagaimana diatur dalam UU PDP. Penggunaan data biometrik seperti wajah dan suara tanpa izin dapat dikategorikan sebagai pelanggaran serius terhadap hak privasi sehingga undang-undang ini berfungsi sebagai instrumen perlindungan preventif terhadap eksploitasi data pribadi dalam pembuatan deepfake.

Dari perspektif hukum pidana umum, KUHP dapat diterapkan apabila perbuatan deepfake memenuhi unsur tindak pidana seperti penipuan, pemerasan, pengancaman, atau pencemaran nama baik.¹⁸ Dalam teori pertanggungjawaban pidana, seseorang dapat dimintai pertanggungjawaban apabila terdapat unsur perbuatan (*actus reus*) dan kesalahan atau kesengajaan (*mens rea*). Pelaku yang dengan sadar menggunakan AI untuk memanipulasi identitas seseorang dan menyebarkannya dengan tujuan memperoleh keuntungan atau merugikan pihak lain telah memenuhi unsur kesengajaan (*dolus*).¹⁹ Dengan demikian, AI dipandang sebagai sarana untuk melakukan tindak pidana dan tidak menghapus pertanggungjawaban pidana pelakunya.

Peraturan Pemerintah Nomor 71 Tahun 2019 mewajibkan penyelenggara sistem elektronik menjamin keamanan, keandalan, dan perlindungan data yang diproses secara elektronik.²⁰ Dalam konteks deepfake, penyelenggara platform digital mempunyai tanggung jawab untuk mencegah penyebaran konten manipulatif yang melanggar hukum. Selanjutnya, Permenkominfo Nomor 5 Tahun 2020 mewajibkan penyelenggara sistem elektronik privat melakukan pengendalian terhadap konten yang dilarang dan memberikan dasar bagi pemerintah untuk meminta penghapusan (*take down*) konten deepfake yang mengandung unsur pelanggaran hukum.

Menurut teori kebijakan hukum pidana yang dikemukakan oleh Barda Nawawi Arief,

¹⁷ Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

¹⁸ Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

¹⁹ Moeljatno, Asas-Asas Hukum Pidana (Jakarta: Rineka Cipta, 2015), hlm. 153–157.

²⁰ Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.



hukum pidana harus mampu menyesuaikan diri dengan perubahan sosial dan perkembangan teknologi.²¹ Ketergantungan pada pasal-pasal umum dalam UU ITE dan KUHP menyebabkan penegakan hukum terhadap *deepfake* bersifat interpretatif dan reaktif. Oleh sebab itu, diperlukan kebijakan hukum pidana yang secara khusus mengatur definisi hukum *deepfake*, larangan pembuatan dan distribusinya yang merugikan, standar pembuktian forensik digital, kewajiban pelabelan (*watermark*) konten hasil AI, serta tanggung jawab platform digital dalam mencegah penyebaran konten manipulatif.

Dari sudut pandang kriminologi siber, penyalahgunaan *deepfake* dapat dijelaskan melalui *Routine Activity Theory* yang menyatakan bahwa kejahatan terjadi ketika terdapat pelaku yang termotivasi, target yang sesuai, dan lemahnya pengawasan.²² Media sosial menyediakan target yang mudah diakses, sementara teknologi AI memungkinkan pelaku melakukan manipulasi dengan biaya rendah dan jangkauan yang luas. Karakter *borderless* dari kejahatan siber menyebabkan pelaku dapat menggunakan server luar negeri dan identitas anonim sehingga menyulitkan proses pelacakan. Hal ini menunjukkan bahwa *deepfake* merupakan bentuk kejahatan siber generasi baru yang memerlukan pendekatan multidisipliner antara hukum pidana, teknologi informasi, dan forensik digital.

Berdasarkan uraian tersebut, dapat dipahami bahwa pengaturan hukum terhadap penyalahgunaan AI melalui teknologi *deepfake* di Indonesia masih bersifat parsial dan tersebar dalam berbagai regulasi. UU ITE memberikan dasar pemidanaan dan pengakuan alat bukti elektronik melalui Pasal 5, UU PDP melindungi data pribadi yang digunakan untuk pelatihan AI, KUHP mengatur tindak pidana umum seperti penipuan dan pencemaran nama baik, sedangkan PP Nomor 71 Tahun 2019 dan Permenkominfo Nomor 5 Tahun 2020 memberikan dasar pengawasan terhadap penyelenggara sistem elektronik. Namun, dari perspektif teori negara hukum, hak asasi manusia, pertanggungjawaban pidana, kebijakan hukum pidana, dan kriminologi siber, regulasi yang ada belum sepenuhnya mampu menjawab kompleksitas kejahatan berbasis AI. Oleh karena itu, pembentukan undang-undang khusus mengenai AI dan *deepfake* menjadi kebutuhan

²¹ Barda Nawawi Arief, *Kebijakan Hukum Pidana* (Jakarta: Kencana, 2018), hlm. 45–49.

²² Larry J. Siegel, *Criminology: Theories, Patterns, and Typologies* (Boston: Cengage Learning, 2018), hlm. 221–223.

mendesak untuk memberikan kepastian hukum, perlindungan hak asasi manusia, dan efektivitas penegakan hukum terhadap tindak pidana siber berbasis kecerdasan buatan.

Penegakan Hukum pada Direktorat Reserse Siber Polda Sumatera Utara

Penegakan hukum terhadap tindak pidana yang menggunakan teknologi *deepfake* di Direktorat Reserse Siber Polda Sumatera Utara merupakan bagian dari upaya penanggulangan kejahatan siber yang semakin berkembang seiring dengan kemajuan *Artificial Intelligence* (AI). Kejahatan berbasis *deepfake* memiliki karakteristik khusus, yaitu dilakukan melalui media digital, dapat menggunakan identitas anonim, dan sering melintasi batas yurisdiksi negara, sehingga membutuhkan metode penanganan yang tidak hanya mengandalkan teknik penyidikan konvensional, tetapi juga dukungan teknologi forensik digital dan koordinasi lintas lembaga.²³

Ditinjau dari teori kewenangan kepolisian, tindakan penyelidikan dan penyidikan yang dilakukan Direktorat Reserse Siber Polda Sumatera Utara merupakan kewenangan atributif yang diberikan secara langsung oleh undang-undang kepada Kepolisian Negara Republik Indonesia. Dalam konsep atribusi, kewenangan tersebut melekat pada institusi kepolisian sebagai organ negara yang bertugas memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan kepada warga negara.²⁴ Dengan demikian, aktivitas seperti penelusuran jejak digital, identifikasi akun, dan penyitaan barang bukti elektronik merupakan pelaksanaan kewenangan yang sah menurut ketentuan hukum yang berlaku.

Menurut teori penegakan hukum yang dikemukakan Soerjono Soekanto, keberhasilan penegakan hukum ditentukan oleh lima unsur, yaitu substansi hukum, aparat penegak hukum, sarana dan prasarana, masyarakat, serta budaya hukum.²⁵ Dalam perkara *deepfake*, aspek substansi hukum tercermin dari belum adanya regulasi khusus yang secara komprehensif mengatur penyalahgunaan AI. Dari sisi aparat penegak hukum,

²³ Rudi Hartono, "Pembuktian Forensik Digital pada Tindak Pidana Siber," Jurnal Yudisial 17, no. 1 (2024): 55–72.

²⁴ Ridwan HR, Hukum Administrasi Negara (Jakarta: RajaGrafindo Persada, 2020), hlm. 101–105.

²⁵ Soerjono Soekanto, Faktor-Faktor yang Mempengaruhi Penegakan Hukum (Jakarta: RajaGrafindo Persada, 2019), hlm. 8–10.



tantangan muncul karena jumlah penyidik yang memiliki keahlian di bidang forensik AI masih terbatas. Sementara itu, sarana dan prasarana berkaitan dengan kebutuhan laboratorium forensik digital yang lebih modern, sedangkan faktor masyarakat dan budaya hukum terlihat dari rendahnya literasi digital serta kebiasaan menyebarkan informasi tanpa proses verifikasi.

Proses penegakan hukum diawali dengan penerimaan laporan masyarakat mengenai dugaan penyalahgunaan konten digital. Setelah itu dilakukan penyelidikan digital untuk mengidentifikasi akun, perangkat, alamat IP, dan jejak elektronik lainnya yang berkaitan dengan pelaku. Pada tahap ini penyidik memanfaatkan teknologi digital tracing dan open source intelligence (OSINT) guna menelusuri sumber penyebaran konten. Apabila ditemukan indikasi manipulasi berbasis AI, penyidik kemudian melakukan analisis forensik digital dengan membandingkan metadata, pola piksel gambar, audio fingerprint, dan karakteristik suara asli dengan hasil rekayasa AI.²⁶

Dari perspektif teori pembuktian, penanganan perkara deepfake berkaitan erat dengan sistem pembuktian negatif menurut undang-undang yang dianut dalam hukum acara pidana Indonesia. Hakim tidak cukup hanya memperoleh keyakinan, tetapi keyakinan tersebut harus didukung oleh alat bukti yang sah menurut undang-undang. Dalam konteks ini, Pasal 5 UU ITE yang mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah menjadi dasar penting bagi penggunaan hasil analisis forensik digital dalam persidangan.²⁷ Selain itu, integritas barang bukti elektronik harus dijaga melalui mekanisme *chain of custody* sejak penyitaan hingga pemeriksaan di pengadilan agar kekuatan pembuktiannya tidak diragukan.

Penegakan hukum terhadap deepfake juga harus dipahami melalui teori sistem peradilan pidana terpadu (*integrated criminal justice system*). Penanganan perkara tidak dapat dilakukan secara parsial oleh kepolisian saja, tetapi membutuhkan koordinasi dengan Kementerian Komunikasi dan Digital, Badan Siber dan Sandi Negara (BSSN),

²⁶ Yuniarti, "Efektivitas Penegakan Hukum terhadap Kejahatan Siber di Indonesia," Jurnal Mimbar Hukum 36, no. 2 (2024): 267–283

²⁷ Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

kejaksaan, pengadilan, serta penyelenggara sistem elektronik.²⁸ Kerja sama tersebut diperlukan untuk memperoleh data teknis, melakukan penghapusan (*take down*) konten yang melanggar hukum, serta memastikan bahwa proses penyidikan, penuntutan, dan pemeriksaan di pengadilan berjalan secara terintegrasi.

Dalam kerangka kebijakan hukum pidana, penanganan deepfake harus mengombinasikan pendekatan preventif dan represif. Pendekatan preventif dilakukan melalui peningkatan literasi digital masyarakat, pengawasan terhadap penyelenggara sistem elektronik, pemberian label pada konten hasil AI, serta pengembangan sistem deteksi otomatis terhadap konten sintesis. Adapun pendekatan represif dilaksanakan melalui penyelidikan, penyidikan, penyitaan barang bukti digital, penuntutan, dan pemidanaan terhadap pelaku yang terbukti menyalahgunakan teknologi AI.²⁹ Penggabungan kedua pendekatan tersebut penting karena pemidanaan saja tidak akan efektif apabila distribusi konten manipulatif tetap berlangsung tanpa pengawasan yang memadai.

Dari sudut pandang hukum progresif yang dikembangkan oleh Satjipto Rahardjo, hukum harus mampu bergerak mengikuti kebutuhan masyarakat dan tidak boleh terjebak pada keterbatasan teks peraturan.³⁰ Oleh sebab itu, ketiadaan undang-undang khusus mengenai deepfake tidak dapat dijadikan alasan untuk membiarkan pelanggaran hukum terjadi. Aparat penegak hukum dituntut melakukan penafsiran yang progresif terhadap ketentuan yang ada agar perlindungan terhadap korban dan ketertiban ruang digital dapat diwujudkan secara efektif.

Secara keseluruhan, penegakan hukum terhadap deepfake di Direktorat Reserse Siber Polda Sumatera Utara menunjukkan adanya pergeseran dari pola penegakan hukum konvensional menuju penegakan hukum digital (*digital law enforcement*). Keberhasilan penanganan perkara tidak lagi hanya ditentukan oleh kemampuan penyidik memeriksa saksi dan tersangka, tetapi juga oleh kemampuan menganalisis data elektronik,

²⁸ Muladi, *Kapita Selekta Sistem Peradilan Pidana* (Semarang: Badan Penerbit Universitas Diponegoro, 2002), hlm. 15–18.

²⁹ Barda Nawawi Arief, *Kebijakan aHukum Pidana* (Jakarta: Kencana, 2018), hlm. 45–49.

³⁰ Satjipto Rahardjo, *Hukum Progresif: Hukum yang Membebaskan* (Jakarta: Kompas, 2009), hlm. 67–70.

memahami mekanisme kerja algoritma AI, menjaga integritas alat bukti digital, dan membangun koordinasi dalam sistem peradilan pidana terpadu. Oleh karena itu, peningkatan kualitas sumber daya manusia, modernisasi laboratorium forensik digital, dan pembentukan regulasi khusus mengenai AI dan *deepfake* menjadi kebutuhan yang mendesak untuk meningkatkan efektivitas penegakan hukum di Indonesia.

Kendala dan Faktor dalam Penanganan Tindak Pidana Deepfake

Hasil penelitian menunjukkan bahwa Direktorat Reserse Siber Polda Sumatera Utara menghadapi berbagai hambatan dalam menangani tindak pidana yang menggunakan teknologi *deepfake*. Hambatan tersebut tidak hanya berkaitan dengan aspek teknis, tetapi juga menyangkut persoalan regulasi, kapasitas kelembagaan, yurisdiksi, dan tingkat kesadaran hukum masyarakat. Hal ini menunjukkan bahwa penanganan *deepfake* merupakan persoalan hukum pidana modern yang membutuhkan pendekatan yang lebih luas daripada sekadar pendekatan teknologi.

Hambatan pertama berkaitan dengan belum adanya regulasi khusus yang mengatur penyalahgunaan AI dan *deepfake*. Aparat penegak hukum masih menggunakan ketentuan umum dalam UU ITE dan KUHP sebagai dasar penindakan.³¹ Dari sudut pandang doktrin hukum pidana, kondisi tersebut menimbulkan persoalan terkait asas legalitas (*nullum crimen sine lege*) yang menuntut adanya pengaturan yang jelas mengenai perbuatan yang dapat dipidana.³² Ketidakjelasan pengaturan khusus berpotensi menimbulkan perbedaan penafsiran dalam penerapan hukum dan mengurangi kepastian hukum.

Hambatan kedua adalah kesulitan dalam pembuktian forensik digital. Teknologi *deepfake* semakin canggih sehingga hasil manipulasi gambar, suara, dan video sulit dibedakan dari konten asli, terutama pada rekaman dengan kualitas tinggi.³³ Dalam teori pembuktian, alat bukti elektronik harus memenuhi unsur keaslian, integritas, dan reliabilitas. Oleh karena itu, penyidik harus mampu memastikan bahwa hasil analisis

³¹ Dian Eka Putri, "Kekosongan Hukum terhadap Penyalahgunaan Artificial Intelligence dalam Tindak Pidana Siber," *Jurnal Arena Hukum* 17, no. 2 (2024): 201–219.

³² Andi Hamzah, *Asas-Asas Hukum Pidana* (Jakarta: Rineka Cipta, 2017), hlm. 39–41.

³³ Kevin R. Johnson, "Deepfake Detection and Digital Evidence Challenges," *International Journal of Digital Forensics* 12, no. 1 (2024): 44–58.

forensik benar-benar menunjukkan adanya rekayasa AI dan dapat dipertanggungjawabkan secara hukum.

Hambatan ketiga berkaitan dengan keterbatasan sumber daya manusia. Jumlah penyidik yang memiliki kompetensi di bidang AI dan forensik digital masih relatif sedikit dibandingkan dengan meningkatnya kasus kejahatan siber.³⁴ Dalam teori penegakan hukum, kualitas aparat penegak hukum merupakan faktor penting yang menentukan keberhasilan penegakan hukum. Tanpa peningkatan kemampuan teknis, penyidik akan mengalami kesulitan dalam mengidentifikasi metode manipulasi AI yang terus berkembang.

Hambatan keempat adalah karakter lintas batas kejahatan siber. Pelaku sering menggunakan server yang berada di luar negeri, identitas anonim, dan platform digital yang beroperasi di luar yurisdiksi nasional.³⁵ Dari perspektif doktrin yurisdiksi pidana, kondisi ini menimbulkan persoalan mengenai kewenangan negara untuk menindak pelaku yang berada di wilayah hukum lain. Penanganan perkara deepfake sering memerlukan kerja sama internasional melalui mekanisme mutual *legal assistance* dan pertukaran data lintas negara.

Hambatan kelima adalah rendahnya literasi digital masyarakat. Banyak pengguna internet belum mampu membedakan antara konten asli dan konten hasil rekayasa AI sehingga mudah menjadi korban penipuan, pemerasan, maupun penyebaran informasi palsu.³⁶ Dalam perspektif kebijakan hukum pidana, kondisi tersebut menunjukkan bahwa penanggulangan deepfake tidak cukup dilakukan melalui pemidanaan, tetapi juga memerlukan langkah preventif berupa edukasi dan peningkatan literasi digital masyarakat.

Apabila dianalisis menggunakan teori tujuan pemidanaan, berbagai hambatan tersebut dapat menghambat tercapainya tujuan pemidanaan, baik yang bersifat pembalasan (*retributive*) maupun pencegahan (*preventive*). Ketika pelaku sulit

³⁴ Rina Mulyani, "Kapasitas Penyidik dalam Penanganan Kejahatan Siber Berbasis AI," Jurnal Hukum dan Teknologi 6, no. 1 (2025): 88–102.

³⁵ Jonathan Clough, *Principles of Cybercrime*, 2nd ed. (Cambridge: Cambridge University Press, 2015), hlm. 312–318.

³⁶ Fajar Nugroho, "Literasi Digital sebagai Instrumen Pencegahan Kejahatan Siber," Jurnal Komunikasi dan Informatika 11, no. 3 (2024): 145–159

diidentifikasi atau kesalahannya tidak dapat dibuktikan secara meyakinkan, efek jera terhadap pelaku maupun masyarakat menjadi kurang optimal. Selain itu, lemahnya regulasi dan keterbatasan kapasitas penegak hukum dapat mengurangi kepercayaan masyarakat terhadap kemampuan negara dalam memberikan perlindungan dari ancaman kejahatan berbasis AI.

Dari sudut pandang hukum progresif, berbagai hambatan tersebut tidak seharusnya menjadi alasan untuk menghentikan proses penegakan hukum. Hukum harus mampu menyesuaikan diri dengan perkembangan teknologi dan memberikan perlindungan yang efektif bagi masyarakat meskipun pengaturan khusus belum terbentuk secara sempurna.³⁷ Oleh karena itu, aparat penegak hukum dituntut untuk melakukan penafsiran yang progresif terhadap ketentuan yang ada sambil mendorong pembentukan regulasi baru yang lebih responsif terhadap perkembangan AI.

Untuk mengatasi berbagai hambatan tersebut, diperlukan beberapa langkah strategis, antara lain pembentukan regulasi khusus mengenai AI dan deepfake, peningkatan kapasitas penyidik melalui pelatihan forensik digital dan analisis AI, penguatan kerja sama internasional dalam pelacakan pelaku dan pertukaran data digital, serta peningkatan literasi digital masyarakat agar mampu mengenali dan memverifikasi konten yang beredar di ruang siber. Pendekatan yang menggabungkan aspek normatif, teknis, kelembagaan, dan edukatif diharapkan dapat meningkatkan efektivitas penegakan hukum terhadap tindak pidana deepfake di Indonesia.

4. Penutup

Berdasarkan hasil penelitian, dapat disimpulkan sebagai berikut:

- a. Pengaturan hukum terkait penyalahgunaan Artificial Intelligence melalui teknologi deepfake di Indonesia masih tersebar dalam beberapa peraturan, antara lain Pasal 27, Pasal 28, Pasal 35, dan Pasal 5 UU ITE, ketentuan perlindungan data biometrik dalam UU Pelindungan Data Pribadi, serta pasal-pasal mengenai penipuan, pemerasan, dan pencemaran nama baik dalam KUHP. Walaupun ketentuan tersebut dapat dijadikan

³⁷ Satjipto Rahardjo, *Penegakan Hukum Progresif* (Jakarta: Kompas, 2010), hlm. 52–55.

dasar untuk menindak pelaku, hingga saat ini belum ada undang-undang khusus yang mengatur definisi deepfake, larangan pembuatan dan penyebaran konten sintetis yang merugikan, standar pembuktian forensik digital, maupun tanggung jawab platform digital atas konten berbasis AI.

b. Penegakan hukum oleh Direktorat Reserse Siber Polda Sumatera Utara dilakukan melalui tahapan penerimaan pengaduan masyarakat, penyelidikan digital untuk menelusuri akun dan alamat IP, pemeriksaan forensik elektronik terhadap metadata, pola piksel, dan audio fingerprint, pelacakan pelaku melalui kerja sama dengan penyelenggara sistem elektronik dan penyedia layanan internet, serta penyidikan berdasarkan ketentuan UU ITE dan KUHP. Dalam beberapa kasus, pembuktian dilakukan dengan membandingkan rekaman asli dengan konten hasil manipulasi AI guna memastikan adanya rekayasa digital.

c. Hambatan utama yang dihadapi Direktorat Reserse Siber Polda Sumatera Utara mencakup belum adanya regulasi khusus mengenai AI dan deepfake, kesulitan membedakan konten asli dengan hasil manipulasi AI beresolusi tinggi, keterbatasan penyidik yang memiliki kompetensi forensik AI, penggunaan server luar negeri dan identitas anonim oleh pelaku, serta rendahnya literasi digital masyarakat dalam mengenali konten deepfake. Oleh sebab itu, diperlukan pembentukan regulasi khusus mengenai AI dan deepfake, peningkatan kemampuan penyidik melalui pelatihan forensik digital dan analisis AI, penguatan kerja sama internasional dalam pelacakan pelaku, serta pengembangan program literasi digital yang berkesinambungan bagi masyarakat.

DAFTAR PUSTAKA

A. Buku

- Amiruddin, & Asikin, Z. (2019). Pengantar metode penelitian hukum. RajaGrafindo Persada.
- Arief, B. N. (2018). Kebijakan hukum pidana. Kencana.
- Asshiddiqie, J. (2010). Konstitusi dan konstiusionalisme Indonesia. Sinar Grafika.
- Clough, J. (2015). Principles of cybercrime (2nd ed.). Cambridge University Press.



- Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat di Indonesia*. Bina Ilmu.
- Hamzah, A. (2017). *Asas-asas hukum pidana*. Rineka Cipta.
- Marzuki, P. M. (2021). *Penelitian hukum*. Kencana.
- Moeljatno. (2015). *Asas-asas hukum pidana*. Rineka Cipta.
- Muladi. (2002). *Kapita selekta sistem peradilan pidana*. Badan Penerbit Universitas Diponegoro.
- Rahardjo, S. (2009). *Hukum progresif: Hukum yang membebaskan*. Kompas.
- Rahardjo, S. (2010). *Penegakan hukum progresif*. Kompas.
- Ridwan HR. (2020). *Hukum administrasi negara*. RajaGrafindo Persada.
- Siegel, L. J. (2018). *Criminology: Theories, patterns, and typologies*. Cengage Learning.
- Soekanto, S. (2019). *Faktor-faktor yang mempengaruhi penegakan hukum*. RajaGrafindo Persada.
- Soekanto, S., & Mamudji, S. (2018). *Penelitian hukum normatif: Suatu tinjauan singkat*. RajaGrafindo Persada.
- Widodo. (2013). *Hukum pidana di bidang teknologi informasi cybercrime law*. Aswaja Pressindo.

B. Artikel Ilmiah/ Jurnal

- Fadli, M. (2024). Deepfake sebagai ancaman baru dalam sistem hukum pidana digital. *Jurnal Legislasi Indonesia*, 21(4), 511–528.
- Hartono, R. (2024). Pembuktian forensik digital pada tindak pidana siber. *Jurnal Yudisial*, 17(1), 55–72.
- Johnson, K. R. (2024). Deepfake detection and digital evidence challenges. *International Journal of Digital Forensics*, 12(1), 44–58.
- Mulyani, R. (2025). Kapasitas penyidik dalam penanganan kejahatan siber berbasis AI. *Jurnal Hukum dan Teknologi*, 6(1), 88–102.
- Nasution, F. (2024). Kebijakan hukum pidana terhadap kejahatan siber berbasis artificial intelligence. *Jurnal Penelitian Hukum De Jure*, 24(2), 189–204.
- Nugroho, F. (2024). Literasi digital sebagai instrumen pencegahan kejahatan siber. *Jurnal Komunikasi dan Informatika*, 11(3), 145–159.



Putri, D. E. (2024). Kekosongan hukum terhadap penyalahgunaan artificial intelligence dalam tindak pidana siber. *Jurnal Arena Hukum*, 17(2), 201–219.

Rizki, A. (2024). Pertanggungjawaban pidana terhadap manipulasi konten digital berbasis artificial intelligence. *Jurnal Hukum IUS QUIA IUSTUM*, 31(2), 215–230.

Sari, D. K. (2024). Perlindungan hukum terhadap korban deepfake dalam perspektif UU ITE. *Jurnal RechtsVinding*, 13(3), 401–418.

Wahyuni, S. (2024). Analisis teori pemidanaan terhadap tindak pidana siber. *Jurnal Hukum dan Peradilan*, 13(1), 97–114.

Yuniarti. (2024). Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia. *Jurnal Mimbar Hukum*, 36(2), 267–283.

C. Peraturan Perundang-Undangan

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

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

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Privat.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.