Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
6 (2) 2026, Page: 21521-21528

Penanggulangan Kejahatan *AI Deepfake*: Tantangan Pembuktian Digital Berdasarkan KUHAP 25 (UU No. 20 Tahun 2025)

Khaoeirun Nissa

Magister Ilmu Hukum, Fakultas Hukum, Universitas Lampung

Corresponding author e-mail: khaoeirunnnissa@gmail.com

Published: Mei, 2026

ABSTRACT

This study aims to analyze the juridical construction of artificial intelligence deepfake crime within Indonesian criminal law, particularly concerning the qualification of digital fraud, electronic evidence, and the need to strengthen the modern criminal justice system in responding to the development of artificial intelligence-based crime. The research method employed is normative legal research using statutory and conceptual approaches, through analysis of Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana particularly Artide 492 concerning digital fraud, Kitab Undang-Undang Hukum Acara Pidana concerning electronic evidence, and Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Artide 28D paragraph (1), with secondary data sources consisting of primary, secondary, and tertiary legal materials analyzed qualitatively through systematic and teleological interpretation. The results indicate that deepfake crime constitutes a new form of cybercrime characterized by highly realistic digital manipulation that is difficult to distinguish from authentic content and has the potential to be used for fraud, extortion, and dissemination of false information; the use of such technology may fulfill the elements of digital fraud when intentionally conducted to cause economic loss; evidentiary processes in deepfake cases face significant technical challenges due to the complexity of electronic evidence manipulation; and digital forensics plays an important role in identifying digital fabrication through metadata analysis, visual artifacts, and voice pattern examination, thereby requiring a modern criminal justice system modd that is adaptive to the development of digital technology.

Keywords: Crime, AI Deepfake, Criminal Code.

ABSTRAK

Penelitian ini bertujuan untuk menganalisis konstruksi yuridis kejahatan *artificial intelligence deepfake* dalam hukum pidana Indonesia, terkait kualifikasi penipuan digital, pembuktian elektronik, dan kebutuhan penguatan sistem peradilan pidana modern dalam menghadapi perkembangan kejahatan berbasis kecerdasan buatan. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual, melalui analisis terhadap Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana terutama Pasal 492 mengenai penipuan digital, Kitab Undang-Undang Hukum Acara Pidana terkait alat bukti elektronik, dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 28D ayat (1), dengan sumber data sekunder berupa bahan hukum primer, sekunder, dan tersier yang dianalisis secara kualitatif melalui penafsiran sistematis dan teleologis. Hasil penelitian menunjukkan bahwa kejahatan *deepfake* merupakan bentuk baru kejahatan siber dengan karakter manipulasi digital yang sangat realistis sehingga sulit dibedakan dari konten asli dan berpotensi digunakan untuk penipuan, pemerasan, maupun penyebaran informasi palsu; penggunaan teknologi tersebut dapat memenuhi unsur tindak pidana penipuan digital apabila dilakukan secara sengaja untuk menimbulkan kerugian ekonomi; pembuktian perkara *deepfake* menghadapi tantangan teknis tinggi karena kompleksitas manipulasi bukti elektronik; dan digital forensik memiliki peran penting dalam mengidentifikasi rekayasa digital melalui analisis metadata, artefak visual, serta pola suara, sehingga diperlukan modd sistem peradilan pidana modern yang adaptif terhadap perkembangan teknologi digital.

Kata Kunci: Kejahatan, AI Deepfake, KUHP.

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era revolusi industri 4.0 telah membawa perubahan yang sangat signifikan dalam berbagai aspek kehidupan manusia termasuk dalam bidang ekonomi, sosial, budaya, hingga sistem penegakan hukum. Kemajuan teknologi digital yang pesat memberikan berbagai kemudahan dalam aktivitas manusia seperti komunikasi jarak jauh, pertukaran informasi secara cepat, serta efisiensi dalam berbagai sektor pekerjaan. Namun, perkembangan teknologi digital juga menimbulkan berbagai tantangan baru khususnya dalam bentuk kejahatan siber yang semakin kompleks dan sulit dideteksi. Salah satu bentuk kejahatan digital yang saat ini menjadi perhatian global adalah penyalahgunaan teknologi kecerdasan buatan atau *Artificial Intelligence* (AI) dalam pembuatan konten manipulatif yang dikenal dengan istilah deepfake.

Teknologi *deepfake* merupakan salah satu bentuk pemanfaatan kecerdasan buatan yang memungkinkan seseorang untuk memanipulasi atau merekayasa konten digital berupa gambar, suara, maupun video sehingga terlihat atau terdengar sangat realistis. Teknologi *deepfake* bekerja dengan menggunakan algoritma pembelajaran mesin (*machine learning*) khususnya teknik *deep learning* untuk meniru wajah, ekspresi, maupun suara seseorang secara akurat. Teknologi *deepfake* pada awalnya dikembangkan untuk kepentingan positif seperti industri perfilman, pendidikan, dan hiburan digital. Namun, teknologi *deepfake* juga sering disalahgunakan untuk tujuan kriminal seperti penyebaran informasi palsu, pemerasan, pencemaran nama baik, hingga penipuan berbasis rekaman suara atau video palsu.

Fenomena kejahatan berbasis *deepfake* semakin meningkat seiring dengan semakin mudahnya akses terhadap perangkat lunak kecerdasan buatan yang dapat digunakan oleh masyarakat luas. Berbagai aplikasi berbasis AI memungkinkan seseorang untuk membuat rekaman suara atau video palsu hanya dengan menggunakan data audio atau visual yang tersedia di internet. Hal tersebut tentu menimbulkan risiko yang serius terhadap keamanan informasi dan kepercayaan publik terutama ketika teknologi tersebut digunakan untuk meniru suara atau wajah tokoh masyarakat, pejabat publik, maupun individu tertentu guna melakukan tindakan penipuan.

Salah satu bentuk kejahatan yang mulai banyak terjadi adalah penipuan menggunakan rekaman suara atau video hasil kloning AI untuk memanipulasi korban agar melakukan tindakan tertentu seperti mentransfer sejumlah dana kepada pelaku. Pelaku kejahatan dalam beberapa kasus memanfaatkan teknologi *deepfake* untuk meniru suara pimpinan perusahaan, pejabat pemerintah, atau tokoh masyarakat sehingga korban percaya bahwa instruksi tersebut benar-benar berasal dari orang yang bersangkutan. Modus operandi ini semakin berbahaya karena tingkat kemiripan suara atau video yang dihasilkan oleh teknologi AI sangat tinggi sehingga sulit dibedakan dengan rekaman asli.

Kasus penipuan menggunakan teknologi kloning suara AI telah dilaporkan di berbagai negara dan menunjukkan tren peningkatan dalam beberapa tahun terakhir. Para pelaku biasanya memperoleh data suara korban dari rekaman publik, media sosial, atau video yang tersedia di internet. Data tersebut diproses menggunakan teknologi AI untuk menghasilkan rekaman suara yang sangat mirip dengan suara asli. Rekaman tersebut kemudian digunakan untuk menghubungi korban lain misalnya karyawan perusahaan atau anggota keluarga, dengan tujuan meminta transfer dana secara mendesak. Korban tidak menyadari bahwa suara tersebut merupakan hasil manipulasi teknologi sehingga dengan mudah mempercayai permintaan pelaku.

Perkembangan kejahatan berbasis *deepfake* tersebut menimbulkan tantangan baru bagi sistem hukum pidana khususnya dalam hal pembuktian di pengadilan. Alat bukti dalam hukum acara pidana tradisional yang diakui umumnya terbatas pada keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Namun, dalam kejahatan digital yang melibatkan manipulasi teknologi tinggi seperti *deepfake*, pembuktian sering kali membutuhkan analisis teknis yang kompleks termasuk pemeriksaan terhadap sistem elektronik dan data digital yang digunakan dalam pembuatan konten.

Pemerintah Indonesia menyadari perkembangan teknologi dan kompleksitas kejahatan digital sehingga melakukan pembaruan terhadap sistem hukum acara pidana melalui pembentukan KUHAP baru yang diatur dalam Undang-Undang Nomor 20 Tahun 2025. Salah satu perubahan penting dalam KUHAP tersebut adalah pengakuan terhadap informasi elektronik dan sistem elektronik sebagai alat bukti yang sah dalam proses peradilan pidana. Ketentuan tersebut tercantum dalam Pasal 5 ayat (1)

KUHAP 2025 yang memperluas definisi alat bukti sah sehingga mencakup berbagai bentuk data digital yang sebelumnya tidak secara eksplisit diatur dalam KUHAP lama.

Perluasan alat bukti merupakan langkah penting dalam menyesuaikan sistem peradilan pidana dengan perkembangan teknologi informasi. Alat bukti digital diakui sebagai alat bukti yang sah. Aparat penegak hukum memiliki dasar hukum yang lebih kuat untuk menggunakan berbagai bukti digital dalam proses penyidikan, penuntutan, maupun pemeriksaan di pengadilan. Hal tersebut sangat relevan dalam penanganan kasus kejahatan berbasis *deepfake* yang pada dasarnya bergantung pada bukti digital dan analisis teknis terhadap sistem elektronik.

Pelaku penipuan menggunakan teknologi *deepfake* dapat dijerat dengan ketentuan dalam KUHP Nasional khususnya Pasal 492 yang mengatur tentang penipuan digital. Pasal tersebut menyatakan bahwa setiap orang yang dengan sengaja menggunakan teknologi informasi untuk menipu orang lain dengan tujuan memperoleh keuntungan secara melawan hukum dapat dipidana dengan ancaman pidana penjara paling lama empat tahun. Ketentuan tersebut menunjukkan bahwa hukum pidana Indonesia telah mulai mengantisipasi berbagai bentuk kejahatan digital yang muncul akibat perkembangan teknologi.

Penerapan ketentuan hukum pidana terhadap kasus *deepfake* masih menghadapi berbagai kendala terutama dalam aspek pembuktian. Salah satu tantangan utama adalah bagaimana membuktikan bahwa rekaman suara atau video yang digunakan oleh pelaku merupakan hasil manipulasi teknologi AI dan bukan rekaman asli. Hal tersebut memerlukan keahlian khusus dalam bidang digital forensik untuk menganalisis struktur data digital, meta data, dan algoritma yang digunakan dalam pembuatan konten. Digital forensik merupakan cabang ilmu forensik yang berfokus pada identifikasi, pengumpulan, analisis, dan penyajian bukti digital dalam proses hukum.

Ahli digital forensik dapat melakukan berbagai metode analisis untuk mendeteksi tanda-tanda manipulasi dalam rekaman suara atau video seperti ketidaksesuaian pola gelombang suara, anomali dalam struktur piksel gambar, maupun perbedaan metadata file digital. Hasil analisis ahli digital forensik kemudian dapat digunakan sebagai alat bukti ilmiah yang membantu hakim dalam menentukan kebenaran materiil dalam suatu perkara pidana. Peran digital forensik dalam sistem peradilan pidana modern menjadi semakin penting seiring dengan meningkatnya jumlah kejahatan berbasis teknologi. Bukti digital sering kali menjadi satu-satunya bukti yang dapat digunakan untuk mengungkap identitas pelaku dan modus operandi yang digunakan. Kemampuan aparat penegak hukum dalam mengelola dan menganalisis bukti digital menjadi faktor yang sangat menentukan keberhasilan penegakan hukum.

Kejahatan *deepfake* juga menimbulkan persoalan serius terkait perlindungan hukum bagi korban. Korban penipuan berbasis *deepfake* tidak hanya mengalami kerugian materiil tetapi juga dapat mengalami kerugian immateriil seperti kerusakan reputasi, tekanan psikologis, dan hilangnya kepercayaan terhadap sistem komunikasi digital. Penggunaan teknologi *deepfake* juga dapat digunakan untuk mencemarkan nama baik seseorang dengan menyebarkan video atau rekaman suara palsu yang seolah-olah menunjukkan bahwa orang tersebut melakukan perbuatan tertentu. Perlindungan hukum tersebut tidak hanya berkaitan dengan penjatuhan sanksi terhadap pelaku tetapi juga mencakup upaya pencegahan, penanganan, dan pemulihan bagi korban. Peran negara menjadi sangat penting dalam menciptakan regulasi yang adaptif terhadap perkembangan teknologi dan memastikan bahwa sistem penegakan hukum mampu merespons berbagai bentuk kejahatan baru yang muncul di era digital.

Transformasi sistem peradilan pidana juga menjadi salah satu aspek penting dalam menghadapi tantangan kejahatan digital pada era revolusi industri 4.0. Sistem peradilan modern tidak lagi dapat bergantung sepenuhnya pada metode konvensional, melainkan harus memanfaatkan teknologi informasi untuk meningkatkan efektivitas dan efisiensi proses penegakan hukum. Hal tersebut mencakup penggunaan sistem manajemen perkara berbasis elektronik, pengumpulan bukti digital secara terintegrasi, dan pemanfaatan teknologi analitik dalam proses penyidikan.

Konsep sistem peradilan pidana modern yang berbasis teknologi juga dikenal dengan istilah digital *justice system* atau sistem peradilan digital. Sistem tersebut memungkinkan berbagai tahapan proses hukum mulai dari penyelidikan, penyidikan, penuntutan, hingga persidangan dilakukan dengan dukungan teknologi informasi yang canggih. Proses pembuktian terhadap kejahatan berbasis teknologi dengan adanya sistem peradilan digital seperti *deepfake* dapat dilakukan secara lebih efektif

karena data digital dapat dianalisis dan disajikan secara sistematis di pengadilan. Penerapan sistem peradilan digital juga menimbulkan berbagai tantangan baru seperti kebutuhan akan sumber daya manusia yang memiliki kompetensi di bidang teknologi informasi, perlindungan terhadap keamanan data digital, dan standar prosedur dalam pengelolaan bukti elektronik.

METODE

Penelitian ini menggunakan pendekatan hukum normatif (*normative legal research*) yang bertujuan untuk menganalisis konstruksi yuridis mengenai kejahatan *artificial intelligence deepfake* dalam perspektif hukum pidana Indonesia, khususnya terkait penipuan digital, pembuktian elektronik, dan penguatan sistem peradilan pidana modern dalam menghadapi perkembangan kejahatan berbasis kecerdasan buatan. Penelitian mengedepankan analisis norma hukum positif yang mengatur tindak pidana berbasis teknologi digital, penggunaan alat bukti elektronik, serta mekanisme pertanggungjawaban pidana terhadap pelaku manipulasi konten digital melalui teknologi *deepfake*. Analisis dilakukan terhadap beberapa ketentuan peraturan perundang-undangan, antara lain Dewan Perwakilan Rakyat Republik Indonesia produk hukum Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana khususnya Pasal 492 mengenai penipuan digital, Kitab Undang-Undang Hukum Acara Pidana terkait pengakuan alat bukti elektronik, serta Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 khususnya Pasal 28D ayat (1) mengenai jaminan kepastian hukum yang adil dalam proses penegakan hukum pidana.

Penelitian ini juga menggunakan pendekatan konseptual (*conceptual approach*) dengan menelaah berbagai konsep dan doktrin dalam ilmu hukum pidana yang berkaitan dengan kejahatan siber, pembuktian digital, *digital forensic*, dan transformasi sistem peradilan pidana modern pada era revolusi industri 4.0. Pendekatan konseptual dilakukan untuk memahami karakteristik kejahatan *deepfake* sebagai bentuk baru manipulasi digital yang memiliki kompleksitas tinggi dalam pembuktian serta membutuhkan adaptasi norma hukum terhadap perkembangan teknologi kecerdasan buatan. Penelitian ini bersifat preskriptif-analitis, yaitu menganalisis norma hukum yang berlaku sekaligus merumuskan argumentasi hukum mengenai efektivitas penerapan ketentuan pidana terhadap pelaku kejahatan *deepfake* dalam praktik peradilan pidana. Sumber data dalam penelitian ini berupa data sekunder yang diperoleh melalui studi kepustakaan terhadap bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier yang relevan dengan perkembangan hukum pidana digital.

Seluruh data yang diperoleh kemudian dianalisis secara kualitatif dengan menggunakan metode penafsiran hukum, terutama penafsiran sistematis dan penafsiran teleologis. Penafsiran sistematis dilakukan dengan menempatkan ketentuan mengenai penipuan digital, alat bukti elektronik, dan peran digital forensik dalam satu kesatuan sistem hukum pidana nasional, sedangkan penafsiran teleologis digunakan untuk menilai tujuan pembentukan norma hukum dalam memberikan perlindungan hukum terhadap masyarakat dari penyalahgunaan teknologi *artificial intelligence* melalui kejahatan *deepfake*.

HASIL DAN PEMBAHASAN

Kejahatan AI Deepfake dalam Perspektif Hukum Pidana

Deepfake merupakan teknologi yang memanfaatkan algoritma kecerdasan buatan khususnya *deep learning* untuk memanipulasi gambar, video, maupun suara sehingga menyerupai individu tertentu secara sangat realistis. Teknologi *deepfake* mampu meniru ekspresi wajah, gerakan bibir, serta intonasi suara seseorang sehingga sulit dibedakan antara rekaman asli dan rekaman yang telah dimanipulasi. Teknologi *deepfake* dapat digunakan dalam industri hiburan, perfilman, dan pendidikan. Namun, teknologi *deepfake* juga sering disalahgunakan untuk berbagai tindak kejahatan seperti penipuan, pemerasan, penyebaran informasi palsu, hingga pencemaran nama baik.

Kejahatan *deepfake* merupakan bagian dari *cybercrime* atau kejahatan siber. Kejahatan *deepfake* dilakukan dengan memanfaatkan teknologi informasi dan komunikasi sebagai sarana utama untuk melakukan manipulasi data digital. Modus operandi yang sering terjadi adalah dengan membuat rekaman suara atau video palsu yang menyerupai pejabat, pimpinan perusahaan, atau tokoh masyarakat tertentu untuk kemudian digunakan sebagai alat untuk menipu korban. Karakteristik

utama kejahatan *deepfake* terletak pada kemampuannya dalam menciptakan ilusi realitas digital yang sangat meyakinkan.

Teknologi *deepfake* menggunakan teknik pembelajaran mesin yang mampu meniru pola suara dan ekspresi wajah secara detail. Hal tersebut menyebabkan proses identifikasi keaslian konten digital menjadi jauh lebih sulit. Kejahatan *deepfake* juga memiliki karakteristik transnasional. Teknologi internet memungkinkan pelaku untuk melakukan kejahatan dari lokasi yang berbeda dengan korban. Pelaku dapat menggunakan server luar negeri, identitas anonim, dan jaringan *virtual private network* (VPN) untuk menyembunyikan identitas.

Tindak Pidana Penipuan Digital dalam KUHP Nasional (Pasal 492)

Pengaturan mengenai tindak pidana penipuan mengalami pembaruan melalui KUHP Nasional. Salah satu ketentuan yang relevan dengan kejahatan *deepfake* adalah Pasal 492 KUHP Nasional yang mengatur mengenai penipuan digital. Pasal tersebut pada dasarnya mengatur bahwa setiap orang yang dengan sengaja menggunakan sistem elektronik atau teknologi digital untuk mengelabui orang lain sehingga menimbulkan kerugian ekonomi dapat dipidana dengan ancaman pidana penjara paling lama empat tahun. Ketentuan tersebut menjadi dasar hukum yang penting dalam menjerat pelaku kejahatan yang memanfaatkan teknologi deepfake untuk melakukan penipuan.

Unsur-unsur tindak pidana yang harus dibuktikan dalam kasus penipuan menggunakan rekaman suara atau video hasil kloning AI meliputi beberapa aspek penting :

1. Adanya perbuatan menggunakan teknologi digital atau sistem elektronik sebagai sarana untuk melakukan manipulasi informasi
2. Adanya unsur kesengajaan dari pelaku untuk menipu atau mengelabui korban
3. Adanya akibat berupa kerugian ekonomi yang dialami oleh korban.

Penggunaan teknologi *deepfake* dapat memenuhi unsur-unsur tersebut apabila pelaku secara sadar membuat konten digital palsu dengan tujuan untuk memperoleh keuntungan secara melawan hukum. Misalnya pelaku membuat rekaman suara yang menyerupai pimpinan perusahaan dan kemudian memerintahkan staf keuangan untuk mentransfer sejumlah uang ke rekening tertentu. Rekaman suara palsu tersebut berfungsi sebagai alat manipulasi psikologis yang memanfaatkan kepercayaan korban terhadap identitas pihak yang ditiru. Korban percaya bahwa perintah tersebut benar-benar berasal dari pimpinan perusahaan sehingga tanpa melakukan verifikasi lebih lanjut langsung melakukan transfer dana.

Tantangan Pembuktian Digital dalam Kasus Deepfake Berdasarkan KUHAP Baru

KUHAP tahun 2025 memberikan pembaruan penting terkait dengan alat bukti digital. Salah satu ketentuan yang relevan adalah Pasal 5 ayat (1) yang memperluas definisi alat bukti sah dengan memasukkan informasi elektronik dan sistem elektronik sebagai bagian dari alat bukti yang dapat digunakan dalam proses peradilan. Ketentuan ini merupakan langkah progresif dalam mengakomodasi perkembangan teknologi informasi yang semakin pesat. Bukti digital dalam kejahatan *deepfake* seperti rekaman suara, video, metadata, dan log aktivitas sistem elektronik dapat digunakan sebagai alat bukti dalam proses pembuktian.

Penggunaan bukti digital juga menghadapi berbagai tantangan. Salah satu tantangan utama adalah tingkat manipulasi teknologi yang semakin canggih. Teknologi *deepfake* mampu menghasilkan konten digital yang hampir tidak dapat dibedakan dari rekaman asli oleh manusia biasa. Hal tersebut menyebabkan proses verifikasi keaslian bukti digital menjadi sangat kompleks. Bukti digital dapat dengan mudah disalin, diubah, atau bahkan dihapus tanpa meninggalkan jejak yang jelas. Proses pengumpulan dan pengamanan bukti digital harus dilakukan dengan prosedur yang ketat untuk menjaga integritas data.

Peran Digital Forensik dalam Mengungkap Manipulasi AI Deepfake

Digital forensik merupakan cabang ilmu forensik yang berfokus pada identifikasi, pengumpulan, analisis, dan penyajian bukti digital dalam proses peradilan. Proses digital forensik biasanya dimulai dengan tahap identifikasi sumber bukti digital. Penyidik akan mengidentifikasi perangkat elektronik yang diduga digunakan dalam tindak pidana seperti komputer, telepon seluler,

server, maupun media penyimpanan digital lainnya. Tahap selanjutnya adalah analisis data digital. Analisis dalam kasus *deepfake* dapat dilakukan dengan menggunakan berbagai teknik seperti analisis pola suara, deteksi artefak visual, dan pemeriksaan meta data file digital. Ahli digital forensik melalui teknik tersebut dapat mengidentifikasi tanda-tanda manipulasi yang menunjukkan bahwa suatu rekaman merupakan hasil rekayasa teknologi AI.

Teknologi deteksi *deepfake* juga terus berkembang seiring dengan meningkatnya kompleksitas algoritma AI. Beberapa metode deteksi *deepfake* memanfaatkan analisis inkonsistensi gerakan wajah, ketidaksesuaian pencahayaan, dan pola frekuensi suara yang tidak alami. Hasil analisis digital forensik kemudian disusun dalam bentuk laporan ahli yang dapat digunakan sebagai alat bukti di pengadilan. Laporan tersebut biasanya memuat penjelasan mengenai metode analisis yang digunakan, temuan yang diperoleh, dan kesimpulan mengenai keaslian konten digital yang diperiksa. Digital forensik berfungsi sebagai jembatan antara teknologi dan sistem peradilan pidana. Tanpa adanya dukungan digital forensik yang memadai akan sangat sulit bagi aparat penegak hukum untuk membuktikan kejahatan yang memanfaatkan teknologi *deepfake*.

Model Sistem Peradilan Pidana Modern dalam Penanganan Kejahatan Deepfake

Perkembangan teknologi informasi pada era revolusi industri 4.0 menuntut adanya transformasi dalam sistem peradilan pidana. Sistem peradilan pidana yang konvensional sering kali tidak mampu mengimbangi kompleksitas kejahatan berbasis teknologi digital seperti *deepfake*. Diperlukan model sistem peradilan pidana modern yang mampu mengintegrasikan teknologi digital dalam setiap tahapan proses penegakan hukum. Model sistem peradilan tersebut harus mencakup berbagai aspek mulai dari penyelidikan, penyidikan, penuntutan, hingga proses persidangan di pengadilan.

Salah satu konsep yang berkembang adalah *digital criminal justice system*. Sistem tersebut memanfaatkan teknologi digital untuk meningkatkan efektivitas dan efisiensi proses penegakan hukum. Contohnya adalah penggunaan sistem pelaporan kejahatan secara online, penyimpanan bukti digital dalam database forensik nasional, dan penggunaan teknologi *artificial intelligence* untuk membantu analisis bukti digital. Sistem peradilan pidana modern harus memperkuat kerja sama antar lembaga penegak hukum seperti kepolisian, kejaksaan, pengadilan, dan lembaga forensik digital. Kerja sama antar lembaga penegak hukum sangat penting mengingat penanganan kasus kejahatan digital membutuhkan keahlian multidisipliner yang tidak dapat ditangani oleh satu institusi.

Aspek perlindungan hukum bagi masyarakat juga menjadi perhatian penting dalam model sistem peradilan modern. Negara harus memastikan bahwa masyarakat memiliki perlindungan yang memadai terhadap berbagai bentuk kejahatan digital. Sistem peradilan modern harus mampu menjamin keadilan bagi para pihak yang terlibat dalam proses hukum. Misalnya, individu yang menjadi korban pemalsuan identitas digital juga harus mendapatkan perlindungan hukum yang memadai agar reputasi dan hak-haknya tidak dirugikan oleh penyalahgunaan teknologi. Model sistem peradilan pidana modern pada era revolusi industri 4.0 tidak hanya berfokus pada penegakan hukum semata tetapi juga pada upaya pencegahan, perlindungan korban, dan adaptasi terhadap perkembangan teknologi digital yang terus berkembang.

KESIMPULAN

Kejahatan *artificial intelligence deepfake* merupakan bentuk baru kejahatan siber yang lahir dari perkembangan teknologi kecerdasan buatan dan memiliki karakteristik manipulasi digital yang sangat realistis sehingga sulit dibedakan dari konten asli, serta berpotensi digunakan untuk berbagai tindak pidana seperti penipuan, pemerasan, dan penyebaran informasi palsu. Dalam perspektif hukum pidana Indonesia, penggunaan teknologi *deepfake* untuk menipu korban dapat dikualifikasikan sebagai tindak pidana penipuan digital sebagaimana diatur dalam Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana Pasal 492 karena memenuhi unsur penggunaan sistem elektronik secara sengaja untuk mengelabui pihak lain hingga menimbulkan kerugian ekonomi. Meskipun pembaruan Kitab Undang-Undang Hukum Acara Pidana telah mengakui informasi elektronik sebagai alat bukti yang sah, pembuktian kasus *deepfake* tetap menghadapi tantangan teknis yang tinggi akibat kompleksitas manipulasi digital, sehingga peran digital forensik menjadi sangat

penting untuk mengidentifikasi pola manipulasi melalui analisis metadata, artefak visual, dan karakteristik suara digital. Oleh karena itu, penanganan kejahatan *deepfake* menuntut model sistem peradilan pidana modern yang adaptif terhadap perkembangan teknologi, melalui penguatan kapasitas aparat penegak hukum, integrasi teknologi digital dalam proses pembuktian, serta peningkatan perlindungan hukum bagi masyarakat terhadap penyalahgunaan kecerdasan buatan.

REFERENCES

Alamsyah, Prayudi Juni. "Peran Metode Pembuktian Elektronik dan Digital Forensik dalam Penegakan Hukum Pidana Modern di Indonesia." *Jurnal Impresi Indonesia* 5, no. 3 (2026): 1028-1038.

Ali, Ismail, Rusdi Kadir, and Besse Nur Fatimah. "Implementasi Penggunaan Forensik Digital dalam Penyelidikan dan Penyidikan Tindak Pidana di Polres Wajo." *Legal Journal of Law* 4, no. 2 (2025): 53-66.

Ariani, Nenny Dwi Ariani. "Humanistic Criminal Law Enforcement To Achieve Spiritual Justice." *Journal of Legal, Ethical and Regulatory Issues* 21, no. 2 (2018): 1-4.

Dewi, Putu Riskha Puspita. "Pengaturan Hukum Penyalahgunaan AI (Artificial Intelligence) dalam Peniruan Suara atau Voice Cloning terhadap Tindakan Penipuan." *Politika Progresif: Jurnal Hukum, Politik dan Humaniora* 2, no. 2 (2025): 114-122.

Febriansyah, Ferry Irawan. *Cybercrime: Kejahatan di Balik Layar Digital*. Ponorogo: Penerbit Najaha, 2025.

Fernandes, Yoggy Arif, and Yulia Fatma. "Metode Deep Learning dalam Teknologi Deepfake: Systematic Literature Review." *JATI (Jurnal Mahasiswa Teknik Informatika)* 9, no. 2 (2025): 3403-3410.

Ilham, Muhamad, and Agus Salim. "Efektivitas Penggunaan Alat Bukti Elektronik Dalam Proses Pembuktian Menurut Hukum Acara Pidana." *Paulus Legal Research* 3, no. 1 (2025): 1-13.

Jusafri, Nur Hidayani Alimuddin, and Arnadi Chairunnas. "Disrupsi Teknologi Digital dalam Pelaksanaan Sistem Peradilan Pidana dan Pemenuhan Keadilan Di Indonesia." *Jurnal Kolaboratif Sains* 7, no. 9 (2024): 3551-3560.

Kartadinata, Andriansyah. "Rekonstruksi Delik Pidana dalam Kejahatan Deepfake: Tantangan Pembuktian dan Perlindungan Korban." *MUARA HUKUM: Jurnal Ilmiah Ilmu Hukum dan Administrasi Publik* 2, no. 1 (2026): 36-48.

Marpaung, Uzuan Fajarudin. *Peran dan Fungsi Advokat dalam UU No. 20 Tahun 2025: Panduan Praktis untuk Advokat, Mahasiswa Hukum dan Penegak Hukum Lainnya*. Bekasi: MS Publishing, 2026.

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.

Putri, Ni Putu Martina, Made Sugi Hartono, and I. Dewa Gede Herman Yudiawan. "Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence." *Jurnal Pacta Sunt Servanda* 5, no. 2 (2024): 120-129.

Putri, Yani Heskia, and Pudji Astuti. "Penegakan Hukum Deepfake Di Polda Jawa Timur Sebagai Bentuk Kejahatan Siber." *Indonesian Journal of Contemporary Law* 1, no. 1 (2026): 1-21.

Seveney, Madalaine Christella, Demas Brian Wicaksono, and Irwan Kurniawan Soetijono. "Urgensi Regulasi terhadap Penyalahgunaan Deepfake Berbasis AI (Artificial Intelligence) pada Konten Pornografi." *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum sumpah Pemuda* 31, no. 2 (2025): 97-106.

Shabrina, Amelia Nur. "Bahaya Deepfake Dalam Penyalahgunaan Grok AI Di Platform X Sebagai Bentuk Disinformasi." *Integrative Perspectives of Social and Science Journal* 3, no. 1 (2026): 195-207.

Sudiadi, Muhammad Hikmat. "Implementasi Asas Dominus Litis dalam Sistem Peradilan Pidana Modern di Indonesia." *Journal of Interdisciplinary Legal Perspectives* 1, no. 1 (2024): 1-15.

Tiara, Ade, and Basyarudin Basyarudin. "Penyalahgunaan Teknologi Artificial Intelligence (AI) Sebagai Modus Baru Kejahatan Penipuan Digital Dalam Perspektif Hukum Pidana Di Indonesia." *Legis Nexus: Jurnal Ilmu Hukum* 1, no. 1 (2026): 17-22.

Quratuainniza, Happy Sturaya, and Ema Nurkhaerani. "Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan Deepfake di Indonesia." *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora* 4, no. 1 (2026): 71-87.

Yasinta, Dian Putri. "Analisis Pertanggungjawaban Pidana Terhadap Penipuan Online Melalui Aplikasi Telegram dalam Perspektif Hukum Pidana Siber Indonesia: Penelitian." *Jurnal Pengabdian Masyarakat dan Riset Pendidikan* 4, no. 3 (2026): 15696-15705.