ALADALAH : Jurnal Politik, Sosial, Hukum dan Humaniora
Volume 4 Nomor 1
P-ISSN: 2962-889X; E-ISSN: 2962-8903
DOI: https://doi.org/10.59246/aladalah.v2i4
Tersedia online di: https://ejurnalqarnain.stisnq.ac.id/index.php/ALADALAH

Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan *Deepfake* di Indonesia

Happy Sturaya Quratuainniza[1], Ema Nurkhaerani[2]

[1,2] Fakultas Hukum, Universitas pembangunan Nasional "Veteran" Jakarta
Email: 2210611384@mahasiswa.upnvj.ac.id[1], ema.n@upnvj.ac.id[2]

Alamat: Jl. R.S Fatmawati No. 1, Cilandak, Jakarta Selatan 12450
Korespondensi penulis: 2210611384@mahasiswa.upnvj.ac.id

Abstract. *The advancement of Artificial Intelligence (AI) has significantly reshaped human activities, especially within digital innovation and cybersecurity. Among its emerging applications, deepfake technology capable of creating highly realistic synthetic audio-visual content poses serious ethical and legal issues. While this innovation enhances creative and technological potential, it also presents risks, including misinformation, data breaches, financial fraud, and reputational harm. This study analyzes the legal and social implications of deepfake misuse and proposes an adaptive regulatory framework suited for Indonesia. Using a normative and doctrinal legal approach, the findings indicate that current laws, including the Electronic Information and Transactions Law and the Personal Data Protection Law, have not adequately addressed AI-related challenges. The research recommends establishing comprehensive regulations that ensure developer accountability, strengthen platform oversight, and protect victims. That supports collaboration among government, academia, and the private sector to build a fair and secure digital environment.*

Keywords*: Deepfake; Regulation; Misuse of Information Technology.*

Abstrak. Kemajuan teknologi Kecerdasan Buatan (Artificial Intelligence/AI) telah mengubah berbagai aspek kehidupan, terutama di bidang inovasi digital dan keamanan siber. Salah satu penerapannya yang menimbulkan persoalan hukum dan etika serius adalah teknologi deepfake, yang mampu menghasilkan konten visual dan audio sintetis dengan tingkat realisme tinggi. Penelitian ini mengkaji implikasi hukum serta sosial dari penyalahgunaan teknologi tersebut dan menawarkan kerangka regulasi adaptif yang relevan bagi Indonesia. Melalui pendekatan hukum normatif dan doktrinal, penelitian ini menunjukkan bahwa peraturan yang berlaku, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP), belum sepenuhnya menjangkau isu terkait AI. Oleh karena itu, diperlukan pembentukan regulasi komprehensif yang memperjelas tanggung jawab pengembang, memperkuat pengawasan platform digital, dan menjamin perlindungan bagi korban penyalahgunaan, dengan dukungan kolaboratif antara pemerintah, akademisi, dan sektor swasta untuk menciptakan ekosistem digital yang adil dan aman.

Kata kunci: *Deepfake*; Regulasi; Penyalahgunaan teknologi Informasi.

* Happy Sturaya Quratuainniza, 2210611384@mahasiswa.upnvj.ac.id

LATAR BELAKANG

Dalam era modern yang mengalami perkembangan sangat cepat, kemajuan teknologi telah mengalami transformasi yang signifikan. Berbagai aktivitas yang sebelumnya dilakukan secara konvensional kini telah beralih ke bentuk digital. Seiring bergesernya zaman menuju era digitalisasi, hamper seluruh aspek kehidupan menjadi lebih praktis dan efisien. Berbagai pekerjaan dapat diselesaikan dengan cepat dan efektif. Perkembangan tekonologi informasi yang begitu pesat pada era digital telah memunculkan berbagai inovasi, salah satunya adalah kecerdasan buatan atau *artificial intelligence* (AI). *Deepfake* merupakan salah satu produk dari kecerdasan buatan tersebut. Secara etimologis, istilah *deepfake* berasal dari gabungan kata dalam Bahasa inggris "*deep learning*" dan "*fake*". Sebagai bagian dari AI, *deepfake* memanfaatkan algoritma yang mampu beradaptasi berdasarkan bertambahnya data yang diproses. Teknologi *deep learning* memungkinkan perkembangan perangkat lunak yang dapat menghasilkan kontek *deepfake.* Kata "*fake*" dalam istilah *deepfake* menunjukan bahwa media yang dihasilkan bersifat palsu atau tidak autentik. *Deepfake* mampu memanipulasi fitur wajah seseorang dengan memanfaatkan teknologi kecerdasan buatan. Melalui teknologi ini, seseorang dapat mengganti wajah dalah video, meniru suara dan menciptakan objek tiga dimensi yang tidak lagi akurat atau sesuai dengan kenyataan. Meskipun tkonologi ini menawarkan peluang untuk mengasilkan konten visual yang kreatif, keberadaannya juga membuka potensi penyalahgunaan (Syahirah & Prasetyo, 2025).

Kejahatan siber (*cybercrime*) dapat dipahami sebagai setiap perbuatan yang dilakukan oleh individu, kelompok orang, maupun entitas tertentu yang secara melawan hukum memenfaatkan system computer baik sebagai alat untuk melakukan Tindakan kejahatan maupun sebagai objek dari kejahatan tersebut. Tindakan-tindakan demikian, baik yang bersifat pelanggaran terhadap norma hukum materil maupun formal, pada hakikatnya merupakan bentuk perbuatan yang dilarang dan dianca, sanksi oleh peraturan perundang-undangan yang berlaku. Pada masa kini, perkembangan kejahatan siber semakin kompleks dengan munculnya perangkat lunak berbahaya (*malware*) yang memanfaatkan algoritma *deepfake*.

Jenis kejahatan ini sering digunakan untuk melakukan pencurian identitas, penipuan, serta pencemaran nama baik melalui rekayasa citra dan suara palsu. Teknologi berbasis kecerdasan buatan tersebut berpotensi memperluas bentuk-bentuk kejahatan di masa mendatang seiring dengan pesatnya kemajuan teknologi digital (Novera & Fitrri, 2024).

Kemajuan teknologi informasi dan komunikasi membawa dampak yang bersifat ambivalen bagi masyarakat. Di satu sisi, kemajuan ini memberikan kontribusi positif terhadap peningkatan efisiensi, produktivitas, serta perkembangan kebudayaan dan peradaban manusia. Namun, di sisi lain, kemajuan tersebut juga menimbulkan peluang penyalahgunaan yang dapat berimplikasi pada pelanggaran hukum. Dengan demikian, teknologi informasi dan komunikasi tidak hanya berfungsi sebagai instrument penegakan hukum, etetapi, juga dapat menjadi sarana terjadinya pelanggaran terhadap norma hukum. Transformasi digital yang terjadi secara global telah mengubah perilaku social serta gaya hidup masyarakat modern. Dunia yang semakin terkoneksi menjadikan batas-batas geografis dan budaya seolah hilang, menciptakan ruang intekasi yang lebih luas namun juga rentan terhadao penyalahgunaan teknologi dan kejahatan siber lintas negara (Raharjo, 2002).

Saat ini, Indonesia memiliki Undang-Undang yang dapat digunakan untuk menuntut mereka yang menyalahgunakan teknologi *deepfake*. Pasal 35 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Pasal 27 ayat (1) UU No. 1 Tahun 2024, yang merupakan perubahan kedua dari UU No. 11 Tahun 2008, juga relevan untuk menangani kasus penyalahgunaan teknologi *deepfake*. Namun, perlu digaris bawahi bahwa peraturan saat ini tidak membahas penggunaan AI, terutama *deepfake*. Oleh karena itu, peraturan yang lebih ketat dan komprehensif diperlukan untuk menangani masalah *deepfake.* Peraturan ini harus mengatur tidak hanya mereka yang membuat dan menyebarkan konten *deepfakei,* tetapi juga platform yang digunakan untuk menyebarkan konten tersebut (Rohmawat et al., 2024).

Kejahatan yang berbasis kecerdasan buatan (AI) umumnya melibatkan penggunaan teknologi dengan Tingkat kompleksitas yang tinggi, sehingga memerlukan keahlian yang mendalam untuk proses identifikasi dan dibuktikan secara hukum. Di Indonesia dan berbagai negara lain, keterbatasan sumber daya manusia, infrastruktur, serta teknologi menjadi kendala utama dalam proses penegakan hukum terhadap kejahatan jenis ini. Apparat penegak hukum sering kali tidak memiliki akses terhadap perangkat forensic digital yang memadai, sehingga sulit menangani kasus AI dan serangan siber berskala besar. Selain itu, kejahatan berbasis AI bersifat lintas yurisdiksi karena berlangsung di ruang digital tanpa batas geografis. Pelaku dapat beroperasi dari satu negara, sementara korban dan infrastruktur kejahatan tersebar di wilayah lain. Kondisi ini menuntut hadirnya regulasi yang adaptif dan progresif. Oleh karena itum pembentukan Undang-Undang khusus yang mengatur pemanfaatan, pengembangan, dan tanggung jawab hukum terkait AI menjadi kebutuhan mendesak. Regulasi tersebut harus mencakup mekanisme perlindungan terhadao kejahatan berbasis AI dan strategi penanggulangan kejahatan siber yang semakin kompleks. Selain itu, peningkatan kapasistas apparat penegak hukum melalui Pendidikan dan pelatihan mengenai teknologi AI serta kerja sama dengan pakar, akasemisi, dan sektor wisara diperlukan untuk menciptakan pendekatan yang komprehensif dan efektif dalam menghadapi tantangan tersebut (Burhan, 2025).

Kondisi tersebut menunjukan adanya kesenjangan normatif dan institusional dalam sistem hukum Indonesia. Urgensi penelitian ini terletak pada kebutuhan mendesak untuk merumuskan model regulasi AI yang komprehensif dan responsif terhadap perkembangan teknologi *deepfake*. Penelitian ini tidak hanya penting untuk memperkuat perlindungan hukum bagi masyarakat dari penyalahgunaan AI, tetapi juga mendorong pembentukan ekosistem digital yang aman, etis, dan berkeadilan melalui sinergi antara pemerintah, akademisi, sektor swasta, dan masyarakat sipil.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan hukum normatif sebagai landasan analisis utama, dengan dukungan pendekatan doktrinal untuk menelaah asas,

prinsip, serta norma hukum yang relevan. Pendekatan ini dipilih karena bertujuan untuk menggali, menginterpretasikan, dan menilai ketentuan hukum positif serta doktrin hukum yang berkaitan dengan isu-isu aktual dalam sistem hukum Indonesia (Rijadi, 2016). Dalam proses pengumpulan data, penelitian ini mengandalkan tinjauan pustaka yang berfokus pada norma hukum positif, doktrin hukum, dan temuan penelitian akademis, semuanya bersumber dari dokumen tertulis (Bachtiar, 2021).

Namun demikian, pendekatan normatif memiliki keterbatasan tertentu, terutama karena bersifat konseptual dan lebih menitikberatkan pada analisis tekstual terhadap norma hukum yang berlaku. Pendekatan ini tidak secara langsung menggambarkan realitas empiris di lapangan, sehingga hasil kajiannya cenderung bersifat deskriptif dan membutuhkan dukungan penelitian empiris untuk memperoleh pemahaman yang lebih komprehensif mengenai penerapan hukum dalam praktik. Oleh sebab itu, temuan dari penelitian ini lebih berfungsi sebagai pijakan konseptual dalam pengembangan kebijakan dan perumusan regulasi terkait isu kecerdasan buatan dan teknologi deepfake di Indonesia.

HASIL DAN PEMBAHASAN

Risiko Hukum dan Sosial yang Ditimbulkan dari Penyalahgunaan Teknologi *Deepfake*.

Penyalahgunaan teknologi deepfake menimbulkan tantangan yang signifikan dalam ranah hukum maupun etika. Jenis pelanggaran yang timbul akibat praktik tersebut dapat dikatagorikan berdasarkan ketentuan yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Hukum Pidana (KUHP) yang baru. Kondisi ini memunculkan perdebatan terkait sejauh mana batas-batas hukum yang berlaku mampu mengakomodasi penanganan kasus penyalahgunaan deepfake secara efektif. Tekonoloi deepfake merupakan inovasi kecerdasan buatan yang memungkinkan pembuatan konten audio maupun visual

dengan Tingkat relaisme tinggi melalui peniruan wajah dan suara seseorang secara presisi. Kemajuan ini membawa implikasi social yang signifikan, khususnya dalam ranah kejahatan siber dan menurunya Tingkat kepercayaan masyarakat terhadap keaslian informasi digital. Salah satu dampak yang paling menghkhawatirkan dari teknologi tersebut Adalah potensi penyalahgunaannya untuk tindak penipuan finansial. Dengan kemampuan mereplikasi suara atau citra individu tertentu secra meyakinkan, pelaku kejahatan siber dapat menipu korban untuk melakukan Tindakan yang merugikan secara ekonomi (Fitri et al., 2025). Dampak semacam ini menandakan bahwa teknologi deepfake bukan sekedar isu teknologi, melainkan juga masalah kepercayaan sosial terhadap autentisitas data digital.

Namun, UU ITE belum memberikan definisi yang secara eksplisit mengenai kecerdasan buatan (AI) dalam ketentuan hukumnya. Ketidakjelasan ini kemudian memunculkan beragam pandangan dari berbagai kalangan yang berupaya menafsirkan konsep AI serta mengaitkannya dengan ketentuan yang telah diatur dalam UU ITE. Jika ditinjau dari perspektif regulasi tersebut, AI dapat dikategorikan sebagai agen elektronik, karena baik UU ITE maupun Peraturan Pemerintah Nomor 71 Tahun 2019 sebgai peraturan turunannya, telah menetapkan Batasan-batasan mengenai kewajiban serta tanggung jawab para penyelenggara agen elektronik (Maharani et al., 2025). Salah satu konsekuensi signifikan dari adanya kekosongan atau kesenjangan hukum terkait penggunaan teknologi kecerdasan buatan (AI) ialah lemahnya mekanisme perlindungan terhadap korban, khususnya dalam kasus yang berkaitan dengan kekerasan seksual. Kotban kerap menjadi objek manipulasi media digital, misalnya melalui pembuatan video deepfake yang menampilkan mereka dalam situasi yang bersifat merendahkan dan menimbulkan penderitaan psikologis. Dampak yang dialami tidak hanya berupa tekanan sosial akibat penyebaran konten illegal tersebut, tetapi juga beban pembuktian yang berat untuk menunjukan bahwa materi tersebut tidak autentik dan merupakan hasil rekayasa teknologi (Hernawan et al., 2025). Dampak sosial dari penggunaan teknologi deepfake mengindikasikan bahwa inovasi ini berpotensi menurunkannya kepercayaan public serta mencemarkan reputasi individu dalam ruang sosial (Tsaqif et al., 2024). Fenomena ini menegaskan bahwa persoalan deepfake tidak

hanya menyangkut aspek hukum pidana, tetapi juga menyentuh dimensi epistemik masyarakat modern yakni krisis dalam membedakan kebenaran dan kebohongan.

Eksistensi AI sebagai teknologi yang meniru kemampuan kognitif manusia memiliki sifat ambivalen, layaknya pisau bermata dua. Di satu sisi, AI berperan signifikan dalam membantu manusia menyelesaikan berbagai tugas secara efisien dan efektif. Namun, di sisi lain, kehadirannya juga berpotensi menimbulkan ancaman serius, terutama terkait kemungkinan terjadinya tindak criminal yang melibatkan sistem AI. Teknologi ini memiliki potensi untuk melakukan pelanggaran hukum, baik akibat kemampuan otonom yang dimilikinya maupun karena kelemahan dalam sistem pengendaliannya. Ketiadaan regulasi yang tegas mengenai status hukum AI dan konsep pertanggungjawaban pidananya berpotensi memperburuk keadaan, sebab ketidakpastian hukum tersebut dapat memghambat proses pengambilan keputusan ketika AI terlibat dalam suatu tindakan yang bersifat melanggar hukum (K. T. Wibowo, 2025).

Di luar implikasi sosial dan politik, teknologi deepfake memperkenalkan dimensi inovatif dalam kriminalitas digital, khususmya terkait dengan penipuan keuangan. Inovasi ini memfasilitasi pelaku untuk mereplikasi suara atau penampilan individu dengan presisi yang luar biasa, sehingga daoat dimanfaatkan untuk mengelabui orang pribadi atau etintas bisnis. Pada sejumlah insiden global, rekaman audio deepfake telah diteraapkan untuk menyesatkan pengelola keuangan guna mentransfer dana ke akun pelaku. Pelanggran hukum seperti ini tidak hanya mengakinbatkan kerugian ekonomi yang substansial, tetapi juga merusak reputasi korporasi yang terdampak. Akibatnya, Langkah-langkah pencegahan seperti program edukasi keamanan siber untuk staf perusahaan, peningkatan pemahaman mengenai risiko teknologi tesebut, serta pengembangan mekanisme keamanan di bidang keuangan menjadi imperative. Lebih lanjut, diseminasi materi deepfake melalui platform media sosial memperparah krisis kepercayaan pada data elektonik. Sebagian besar konsumen media sosial mengalami kesulitan dalam mengidentifikasi konten autentik versus yang fabrikasi, yang pada akhirnya meningkatkan sikap skeptis terhadao sumber informasi daring. Situasi ini

diperburuk oleh mekanisme algoritma platform yang cendering mengutamakan materi yang menarik perhatian, seperti deepfake, dikarenakan potensi penyebarannya yang luas. Kondisi ini tidak hanya mengganggu interaksi antara public dan media elektronik, tetapi juga menunrunkan keandalam media sosial sebagai wadah informasi terpercaya (Fadillah & Setiawan, 2025).

Dari perspektif sosial, keberadaan teknologi deepfake meningkatkan potensi penyebaran informasi palsu maupun disinformasi secra massif. Konten video atau audio hasil manipulasi yang menampilkan figure public seolah-olah mengucapkan pernyataan kontroversial dapat dengan mudah menyebar luas di media sosial, menimbulkan keresahan, kebingungan, bahkan potensi konflik horizontal di tengah masyarakat. Dalam ranah poliytik, deepfake kerap dimanfaatkan sebgai instrument propaganda, manipulasi opini public, serta sarana untuk mendiskreditkan lawan politik menjelang pemilihan umun, sehingga mengancam integritas proses demokrasi. Dampak sosial lainnya Adalah menurunnya Tingkat kepercayaan masyarakat terhadao media dan institusi. Ketika public semakin sulit membedakan antara informasi yang autentik dan yang dimanipulasi, kepercyaan terhadap pemberitaan, Lembaga pemerintaham, dan sistem hukum mengalami penurunan yang signifikan. Fenomena ini dekanl dengan istilah liar's dividend, yaitu keuntungan strategis bagi pelaku kejahatan yang dapat menyangkal keaslian bukti visual dengan alasan bahwa konten tersebut hanyalah hasil deepfake. Akibatnya, sistem hukum dan demokrasi menghadapi tantangan serius dalam mempertahankan legitimasi serta stabilitasnya. Lebih jauh, deepfake juga memperkuat polarisasi sosial. Disinformasi yang disebarkan secara sistematis berpotensi memperdalam perpecahan sosial, meningkatkan ketidakpastian, serta mengikis kohesi sosial di masyarakat. Dalam jangka Panjang, ketidakmampuan public untuk membedakan kebenaran dari kebohongan dapat mengerus rasa saling percaya antarwarga maupun terhadap negara. Kondisi ini menjadi semakin berisiko di negara-negara dengan Tingkat literasi digital yang relative lebih rendah, seperti Indonesia (Widjaja, 2025).

Selain itu, teknologi kecerdasan buatan (AI) telah diterapkan dalam stategi yang dikenal sebagai predictive policing, yaitu pendekatan yang bertujuan memperkirakan Lokasi serta waktu terjadinya tindak kejahatan berdasarkan analisis data criminal sebelumnya. Namun demikian, penerapan strategi ini sering kali melampaui batas temuan ilmiah yang telah terverifikasi, sehingga menimbulkan perdebatan mengenai validasi, efektivitas, dan implikasi etis dari metode tersebut. Di sisi lain, praktik anonimitas di ruang siber kerap dimanfaatkan oleh pelaku kejahatan digital seperti pencucian uang, perdagangan narkotika, terorisme, sehingga eksploitasi anak di bawah umur. Melalui pemanfaatan berbagai alat dan sumber daya yang tersedia secara daring, para pelaku dapat berkomunikasi serta bertukar informasi dengan risiko yang relative lebih rendah terhadap pengungkapan identitas pribadi mereka. Kondisi ini menciptakan tantangan signifikan bagi apparat penegak hukum dalam menyeimbangkan antara perlindungan terhadap kebebasan berekspresi, hak privasi, dan kepentingan penegakan hukum untuk mengidentifikasi pelaku kejahatan. Dalam konteks media sosial, anonym memberi peluang bagi pengguna untuk membuat identitas palsu yang digunakan dalam penyebaran informasi menyesatkan atau serangan terhadao individu lain. Mislanya, pada platform seperti Twitter (X), pengguna anonym dapat melakukan tindakan perundungan siber maupun distibusi berita palsu. Selain deepfake, teknologi AI juga digunakan dalam strategi predictive policing, yakni upaya memprediksi lokasi dan waktu terjadinya kejahatan berdasarkan analisis data kriminalitas sebelumnya. Meskipun bertujuan meningkatkan efisiensi penegakan hukum, penerapan strategi ini masih menimbulkan perdebatan mengenai validitas ilmiah dan potensi bias algoritmik yang dapat berujung pada diskriminasi (Darmawan et al., 2025).

Sementara itu, praktik anonimitas di ruang digital turut memperumit penegakan hukum terhadap kejahatan dunia maya, seperti pencucian uang, perdagangan narkotika, terorisme, hingga eksploitasi anak. Penggunaan identitas palsu di platform media sosial juga mendorong maraknya perundungan siber dan penyebaran berita palsu. Upaya pendeteksian akun anonim memang telah

dilakukan, namun tantangan utama terletak pada keterbatasan dalam mengaitkan identitas digital dengan idividu sebenarnya.

Desain Regulasi AI yang Ideal untuk Mencegah Dampak Negatif *Deepfake* Tanpa Menghambat Inovasi.

Dalam era digital saat ini, perkembangan tekonologi merupakan faktor dominan yang mendorong transformasi dalam berbagai produk digital. Penerapan kecerdasan buatan (AI) dan pembelajaran mesin (machine learning) telah menciptakan revolusi signifikan dalam pengembangan serta fungsi produk digital modern. Kedua teknologi tersebut termasuk inovasi utama yang berperan dalam membentuk dan memperkaya ekosistem digital kontemporer. Pemanfaatan AI memungkinkan para pengembang untuk merancang produk digital yang bersifat lebih personalis, adaptif, dan responsive, karena kemampuannya dalam melakukan analisis data secara cepat dan presisi. Sebgai ilustrasi, berbagai aplikasi berbasik personalitas kini menggunkan AI untuk mengenai pola perilaku pengguna dan memberikan rekomendasi yang disesuiakan dengan preferensi individu. Dengan demikian, keberadaan AI diyakini akan membawa perubahan mendasar terhadap karakteristik produk digital maupun terhadap ekosistem digital secra keseluruhan (Sutadi, 2025).

Konten deepfake yang bersifat sensasional atau provokatif sering kali memiliki potensi lebih besar untuk viral karena algoritma media sosial cenderung memprioritaskan penyebaran konten dengan jangkauan tinggi. Fenomena ini memperburuk relasi sebagai sarana komunikasi dan sumber informasi yang dapat diandalkan. Sebagai respons terhadap permasalahan tersebut, diperlukan sinergi antara pemangku kepentingan termasuk pemerintah, penyedia platform digital, serta kalangan akademisi, guna memperkuat pengawasan dan membangun sistem deteksi deepfake yang lebih efektif. Kolaborasi lintas sektor ini diharapkan mampu meningkatkan transparansi dalam pengelolaan konten digital dan memperkuat Upaya mitigasi terhadap penyebaran informasi palsu. Dengan demikian pengembangan teknologi deteksi yang lebih akurat, diharapkan dampak negatif dari

penyebaran konten manipulative dapat diminimalisasi, sekaligus memulihkan kepercayaan masyarakat terhadap ekosistem media digital (Fitri et al., 2025).

Teknologi kecerdasan buatan (AI) kini semakin meluas penerapannya di berbagai sektor, termasuk dalam bidang keaman siber. AI memiliki kemampuan dalam mengidentifikasi pola serangan, menganalisis ancaman secara waktu nyata (real time), serta meningkatkan efektivitas respons terhadap insiden digital, melalui penerapan sistem berbasis AI, mekanisme keamanan dapat secra otomatis mendeteksi aktivitas yang mencurigakan dan mencegah terjadinya pelanggaran sebelym menimbulkan kerugian yang lebih besar. Namun demikian, kemajuan AI juga menimbulkan ptensi risiko baru. Teknologi ini tidak hanya dapat dimanfaatkan untuk memperkuat pertahanan siber, tetapi juga berpotensi disalahgunakan oleh pihak tidak bertanggung jawab untuk melakukan serangan siber yang lebih kompleks dan sulit dilacak. AI dapat digunakan untuk menciptakan serangan phising yang tampak meyakinkan, mengembangkan malware yang mampu menghindari deteksi sistem keamanan, serta menghasilkan konten deepfake yang berpotensi digunkan untuk manipulasi digital. Seiring dengan kemajuan teknologi, para pembuat deepfake dan penyebar disinformasi juga terus mengembangkan teknologi baru untuk menghindari deteksi sistem keamanan. Kondisi ini menimbulkan perdebatan mengenai sejauh mana platform digital harus memikul tanggung jawab dalam melakukan penyaringan dan pengawasan konten daring. Sebagian kalangan menilai bahwa penerapan moderasi konten yang terlalu ketat berpotensi membatasi kebebasan berekspresi. Contohnya, Uni Eropa melalui Digital Services Act (DSA) mewajibkan penyedia platform untuk secara cepat dan transparan menghapus konten illegal. Di Indoneisa, Kementerian Komunikasi dan Informatika (Kominfo) telah menetapkan peraturan yang mengharuskan penghapusan konten yang melanggar hukum dalam jangka waktu tertentu setelah adanya laporan (A. Wibowo & Yulianingsih, 2025).

Secara hakikat, kekosongan norma hukum terkait kecerdasan buatan (AI) dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mencerminkan kompleksitas tantangan yang dihadapi Indonesia, termasuk keterbatasan

infrastruktur hukum serta kurangnya sumber daya manusia yang memiliki pemahaman mendalam terhadap teknologi tersebut. Meskipun pemerintah berupaya memberikan ruang fleksibilitas bagi perkembangan teknologi digital, ketiadaan regulasi yang memadai justru meningkatkan potensi penyalahgunaan AI, seperti penyebaran disinformasi dan pelanggaran privasi individu. Pedoman etika yang ada saat ini belum memiliki kekuatan mengikat secara hukum, sehingga diperlukan pembentukan regulasi khusus yang bersifat tegas dan menyeluruh guna menjamin keamanan, keadilan, serta transparansi dalam penerapan AI. Regulasi semacam ini diharapkan tidak hanya menetapkan prinsip-prinsip dasar penggunaan AI secara etis, tetapi juga mengatur kemungkinkan pengakuan AI sebagai subjek hukum yang memiliki tanggung jawab terhadap hasil tindakannya. Dalam konteks tersbeut, Indonesia perlu mengkasi dan mengambil pembelajaran dari praktik di negara lain dalam merancang kebijkan serta regulasi yang tepat, dengan melibatkan berbagai pemangku kepentingan untuk memastikan pemanfaat AI yang bertanggung jawab. Dengan adanya pengaturan yang jelas mendukung perlindungan masyarakat sekaligus mendorong kemajuan digital yang inklusif dan berkeadilan. Meskipun UU ITE telah mengalami beberapa perubahan sejak diberlakukan pada tahun 2008, peraturan tersebut masih dianggap belum memadai dalam mengakomodasi perkembangan teknologi AI yang berisiko tinggi, seperti deepfake. Hal ini disebabkan oleh beberapa factor utama, antara lain tidak adanya definisi yuridis yang spesifik mengenai deepfake maupun bentuk teknologi AI lainnya, sehinggamenyulitkan apparat penegak hukum dalam menerapkan pasal-pasal yang relevan terhadap kasus-kasus terkait. UU ITE lebih menitikberatkan pada aspek umum mengenai informasi dan transaksi elektronik tanpa secara eksplisit mencakup isu-isu baru yang muncul akibat perkembangan AI, seperti manipulasi media digital dan penyebaran informasi palsu (Respati, 2024).

Secra khusus, Pasal 1 UU ITE dinilai masih belum cukup komprehensif dalam menjelaskan sistem kecerdasan buatan secara spesifik. Oleh karena itu, pasal tersebut sebaiknya diperbaharui dengan memasukkan definisi AI sebagai sistem berbasis mesin yang mampu melakukan fungsi yang memerlukan kecerdasan manusia, seperti analisis data, pengenalan pola, dan pengambilan Keputusan

otomatis. Selanjutnya, perluasan terhadap Pasal 40 dan Pasal 43 juga direkomendasikan dengan menambahkan pasal baru yang menegaskan kewajiban transparansi serta akuntabilitas bagi pengembang dan penyedia layanan AI. Pasal 40A yang diusulkan dapat memuat kewajiban bagi pengembang untuk menyediakan informasi yang terbuka mengenai algoritma, sumber data, serta prosedur evaluasi yang digunakan, disertai dengan penerapan mekanisme transparansi dan perlindungan hak pengguna atas data pribadi. Selain itu, pengembang wajib melakukan audit secara berkala dan meyampaikan hasilnya kepada instansi pemerintahan terkait. Sementara itu, Pasal 43A diusulkan untuk memberikan kewenangan kepada pemerintah dalam melakukan pengawasan terhadap kepatuhan pengembangan terhadap teknis dan proses pemeriksaan berkala. Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi administrative sesuai peraturan perundang-undangan yang berlaku (Respati, 2024).

Oleh karena itu, meskipun AI menawarkan potensi besar dalam peningkatan keamanan siber, penggunaanya memerlukan kerangka regulasi yang tegas dan komprehensif guna mencegah penyalahgunaan. Banyak negara saat ini berupaya mengembangkan standar etika dan regulasi untuk memastikan pemanfaatan AI berlangsung secara aman, bertanggung jawab, dan sejalan dengan prinsip hak asasi manusia. Di sisi lain, tanggung jawab platform digital terhadap penyebaran konten berbahaya termasuk deepfake, hoaks, dan ujaran kebencian, masih menjadi isu yang perlu diperhatikan secra serius. Meskipun berbagai Negara telah menerapkan regulasi untuk mengatasi persoalan tersebut, tantangan dalam implementasi dan pengawasannya tetap menjadi pekerjaan berkelanjutan. Untuk membangun ekosistem digital yang aman, adil, dan beretika, diperlukan kolaborasi antara pemerintah, penyedia layanan digital, serta masyarakat. Regulasi yang diterapkan harus tidak hanya efektif dalam melindungi masyarakat dari ancaman digital, tetaou juga tetap menjamin kebebasan berekspresi dan hak-hak pengguna internet. Melalui penguatan kerangka hukum, pengembangan inovasi teknologi, serta peningkatan literasi digital, diharapkan ruang digital dapat berkembang menjadi lingkungan yang lebih aman, inklusif, dan bermanfaat bagi seluruh pengguna (A. Wibowo & Yulianingsih, 2025).

Kondisi ini menunjukan paradoks mendasar dari perkembangan AI yakni bahwa teknologi yang diciptakan untuk memperkuar keamanan, pada saat bersamaan dapat melemahkan sistem sosial jika tidak diatur secara etis dan hukum yang memadai. Oleh karena itu, penyusunan regulasi tidak cukup bersifat terhadap ancaman, tetapi harus proaktif dan antisipatif. Regulasi seharusnya berperan sebagai instrumen pencegahan, bukan sekedar sarana penindakan setelah terjadi pelanggaran. Indonesia perlu mengadopsi model regulasi yang progrestif dan partisipatif, dengan melibatkan akademisi, sektor swasta, dan masyarakat sipil dalam proses perumusan kebijakan. Contohnya pada Uni Eropa dan Korea selatan menunjukan bahwa keberhasilan regulasi AI bergantung pada keterlibatan multipihak dan kemampuan adaptasi hukum terhadap dinamika teknologi.

KESIMPULAN DAN SARAN

Kemajuan teknologi kecerdasan buatan (Artificial Intelligence/AI), khususnya yang terwujud dalam bentuk deepfake, telah menghasilkan dampak yang bersifat paradoksal terhadap tatanan sosial, politik, dan hukum. Di satu sisi, teknologi ini membuka ruang yang luas bagi akselerasi inovasi digital serta ekspresi kreatif; namun di sisi lain, penyalahgunaannya menghadirkan ancaman signifikan berupa tindak kejahatan siber, penipuan daring, pelanggaran privasi pribadi, dan penyebaran disinformasi yang berpotensi mengikis kepercayaan publik terhadap autentisitas informasi digital. Kondisi tersebut bahkan dapat mengganggu stabilitas sistem demokrasi yang bergantung pada integritas dan kejujuran arus informasi publik. Secara normatif, Indonesia telah memiliki dasar hukum melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Namun demikian, kedua instrumen hukum tersebut belum memberikan pengaturan yang secara spesifik mencakup aspek teknologis, etis, dan tanggung jawab hukum dalam penerapan kecerdasan buatan, termasuk teknologi deepfake. Kekosongan pengaturan tersebut menegaskan perlunya pembentukan kerangka hukum yang lebih komprehensif, fleksibel, dan visioner, yang mampu menyeimbangkan antara perlindungan hak asasi manusia, penerapan prinsip etika digital, dan dukungan terhadap kemajuan inovasi teknologi.

Dalam jangka waktu pendek, pemerintah perlu segera membentuk tim lintas sektoral yang terdiri atas unsur kementerian terkait, akademisi, serta pakar teknologi untuk merumuskan Rancangan Undang-Undang Kecerdasan Buatan. Rancangan tersebut diharapkan memuat definisi hukum AI, kategori tingkat risiko, dan standar etika penggunaannya secara jelas. Revisi parsial terhadap UU ITE juga penting untuk menyesuaikan substansinya dengan perkembangan teknologi digital yang terus berubah. Selanjutnya, dalam jangka menengah, peningkatan kompetensi aparat penegak hukum menjadi prioritas utama. Upaya ini dapat dilakukan melalui pelatihan berkelanjutan di bidang forensik digital, teknik identifikasi konten manipulatif, serta penguatan pemahaman terhadap etika hukum dalam penanganan kasus berbasis AI. Pada tahap ini, sinergi antara pemerintah, lembaga pendidikan tinggi, dan sektor swasta perlu diwujudkan dalam pembentukan Pusat Kompetensi Nasional Keamanan Siber dan Etika Digital sebagai wadah peningkatan kapasitas dan inovasi regulatif.

Sementara itu, penyelenggara platform digital harus diberikan tanggung jawab hukum yang lebih kuat dalam mendeteksi, mengontrol, dan menghapus konten deepfake secara proaktif, serta diwajibkan untuk menyampaikan laporan transparansi publik secara periodik guna memastikan akuntabilitas dalam pengelolaan data dan konten digital. Dalam jangka panjang, diperlukan penguatan kerja sama lintas sektor antara pemerintah, akademisi, dan industri teknologi dalam membangun tata kelola kecerdasan buatan nasional yang selaras dengan prinsip-prinsip etika global, sebagaimana tercermin dalam panduan Ethical AI yang ditetapkan oleh OECD dan UNESCO. Implementasi langkah ini dapat diwujudkan melalui pembentukan lembaga pengawas independen yang memiliki mandat untuk memantau kepatuhan terhadap standar etika, memastikan akuntabilitas pengembang teknologi, serta menjamin perlindungan hukum yang efektif bagi masyarakat.

Selain upaya regulatif, pemberdayaan masyarakat melalui program literasi digital nasional harus diintensifkan guna meningkatkan kesadaran hukum dan kemampuan publik dalam mengenali serta menolak konten manipulatif atau

menyesatkan. Kolaborasi yang erat antara pemerintah, akademisi, sektor swasta, dan masyarakat sipil menjadi prasyarat utama bagi terciptanya ekosistem digital yang aman, transparan, beretika, dan berkeadilan. Dengan demikian, perkembangan kecerdasan buatan dapat diarahkan untuk mendukung kemaslahatan sosial dan kemajuan peradaban manusia, bukan menjadi alat penyalahgunaan kekuasaan ataupun ancaman terhadap nilai-nilai moral dan kemanusiaan.

DAFTAR REFERENSI

Artikel Jurnal

Burhan, W. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *Innovative: Journal Of Social Science Research*, *5*(1), 4. https://j-innovative.org/index.php/Innovative/article/view/17519

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan Hukum Terhadap Penyalahgunaan DeepfakePada Pornografi Anak Di Era Artifical Intelegencedi Indonesia. *Jurnal Serambi Hukum*, *18*(1). https://www.journal.uniba.ac.id/index.php/SH/article/view/1257

Fadillah, N. M. F., & Setiawan, H. (2025). *Dampak Teknologi Deepfake Terhadap Kepercayaan Publik dan Penyebaran Informasi di Media Sosial*. https://www.researchgate.net/profile/Nazar-Muhammad-Fikri-Fadillah/publication/388412074

Fitri, D., Hidayah, A. N., Putri, A., Tanjung, N. H., Ramadhani, S. I., Akila, D., Manurung, R. A., Mufidah, N., Akbar, S., & Zikri, M. (2025). Deepfake dan Krisis Kepercayaan: Analisis Hukum Terhadap Penyebaran Konten Palsu di Media Sosial. *JIIC: Jurnal Intelek Insan Cendikia*, *2*(6). https://doi.org/https://jicnusantara.com/index.php/jiic/article/view/3787

Hernawan, C. N. P., Antow, D. T., & Sendow, A. (2025). Tinjauan Hukum Mengenai Penyalahgunaan Artificial Intelligence dalam Tindak Pidana Kekerasan Seksual. *Lex Privatum*, *15*(5). https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/61860

Maharani, B. A., Rahajeng, H. A., T, T., & Arianti, Z. D. (2025). Perlindungan Hukum Masyarakat dari Dampak Negatif Penggunaan AI. *Jurnal Media Hukum Indonesia (MHI)*, *3*(2). https://ojs.daarulhuda.or.id/index.php/MHI/article/view/1939

Novera, O., & Fitrri, Y. (2024). Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial. *El-Faqih: Jurnal Pemikiran Dan Hukum Islam*, *10*(2), 462. https://doi.org/https://doi.org/10.58401/faqih.v10i2.1539

Raharjo, A. (2002). *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan*

Berteknologi (cet. 1). Citra Aditya Bakti.

Respati, A. A. (2024). Reformulasi Undang-UndangITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropadan ChinaAI Act Regulation. *Jurnal USM Law Review*, *7*(3), 1748. https://doi.org/ttps://doi.org/10.26623/julr.v7i3.10578

Rijadi, J. E. P. (2016). *Metode Penelitian Hukum Normatif dan Empiris*. KENCANA.

Rohmawat, I., Junaidi, A., & Khaerudin, A. (2024). Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO). *Innovative: Journal Of Social Science Research*, *4*(6), 3. https://doi.org/https://doi.org/10.31004/innovative.v4i6.16559

Sutadi, H. (2025). *AI Untuk Negeri: Strategi Inovasi, Regulasi dan Kedaulatan Teknologi Digital Indonesia* (cet. 1). Zifatama Jawara. https://books.google.co.id/books?hl=en&lr=&id=y4yLEQAAQBAJ&oi=fnd&pg=PA1&dq=2.%09

Syahirah, S. N., & Prasetyo, B. (2025). Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake untuk Pornografi Melalui Artificial Intelligence (AI) di Indonesia. *Jurnal Inovasi Hukum Dan Kebijakan*, *6*(1), 192. https://ejurnals.com/ojs/index.php/jihk/article/view/1405

Widjaja, G. (2025). Deepfake dan Masa Depan Kebenaran: Implikasi Etis dan Sosial. *Berajah Journal*, *5*(2), 152. https://ojs.berajah.com/index.php/go/article/view/591

Buku Teks

Bachtiar. (2021). *Mendesain Penelitian Hukum*. Deepublish.

Wibowo, A., & Yulianingsih, S. (2025). *Hukum Teknologi Informasi*. Yayasan Prima Agus Teknik. https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/578/604

Wibowo, K. T. (2025). *Aspek Hukum dalam Dunia Digital*. Sada Kurnia Pustaka. https://books.google.co.id/books?hl=en&lr=&id=MeB2EQAAQBAJ&oi=fnd&pg=PA118&dq=1.

Disertasi/Tesis/Paper Kerja

Tsaqif, D. N. A., Rajata, M. R., Hassan, T. K., & Rakhmawati, N. A. (2024). *Penggunaan Teknologi Deepfake: Analisis Kesadaran Etis di Kalangan Mahasiswa ITS* [Institut Teknologi Sepuluh Nopember]. https://www.researchgate.net/profile/Dia-Tsaqif/publication/381842733_Penggunaan_Teknologi_Deepfake_Analisis_Kesadaran_Etis_di_Kalangan_Mahasiswa_ITS/links/66815b182aa57f3b82614a22/Penggunaan-Teknologi-Deepfake-Analisis-Kesadaran-Etis-di-Kalangan-Mahasiswa-ITS.pdf