ALADALAH : Jurnal Politik, Sosial, Hukum dan Humaniora
Volume 3 Nomor 2 April 2025
P-ISSN: 2962-889X; E-ISSN: 2962-8903, Hal 149-164
DOI: https://doi.org/10.59246/aladalah.v2i4
Tersedia online di: https://ejurnalqarnain.stisnq.ac.id/index.php/ALADALAH

Pencegahan Kejahatan *Deepfake*: Studi Kasus terhadap Modus Penipuan *Deepfake* Prabowo Subianto dalam Tawaran Bantuan Uang

Yoan Shevila Kristiyenda[1*], Jasmine Faradila[2], Christina Basanova[3]
[1-3] Universitas Padjadjaran, Indonesia
Korespondensi penulis: yoan21001@mail.unpad.ac.id

Abstract. *Deepfake has become a serious threat in cybercrime, allowing perpetrators to deceive the public with highly realistic video and audio manipulation. This research aims to analyze the mode of cybercrime that utilizes deepfake technology, especially in cases of fraud involving manipulation of the faces of public figures. This study uses the literature study method by reviewing regulations related to cybersecurity, deepfake technology, and policies that have been implemented in various countries in dealing with this threat. The results indicate that the deepfake crime mode is growing by utilizing public trust in the faked figures. Despite the implementation of several regulations, early detection, law enforcement, and victim protection continue to face challenges. Therefore, stricter and more adaptive policies are needed, along with strengthening cooperation between the government and digital platforms and increasing public digital literacy, to reduce the risk of deepfake crime in the cyber domain.*

Keywords: *Deepfake, Cybercrime, Regulation, Digital Literacy*

Abstrak. *Deepfake* telah menjadi ancaman serius dalam kejahatan siber, memungkinkan pelaku untuk menipu masyarakat dengan manipulasi video dan audio yang sangat realistis. Penelitian ini bertujuan untuk menganalisis modus kejahatan siber yang memanfaatkan teknologi *deepfake*, khususnya dalam kasus penipuan yang melibatkan manipulasi wajah tokoh publik. Studi ini menggunakan metode studi literatur dengan mengkaji regulasi terkait keamanan siber, teknologi *deepfake*, serta kebijakan yang telah diterapkan di berbagai negara dalam menangani ancaman ini. Hasil penelitian menunjukkan bahwa modus kejahatan *deepfake* semakin berkembang dengan memanfaatkan kepercayaan publik terhadap tokoh yang dipalsukan. Meskipun beberapa regulasi telah diterapkan, masih terdapat tantangan dalam deteksi dini, penegakan hukum, serta perlindungan terhadap korban. Oleh karena itu, diperlukan kebijakan yang lebih ketat dan adaptif, penguatan kerja sama antara pemerintah dan platform digital, serta peningkatan literasi digital masyarakat untuk mengurangi risiko kejahatan *deepfake* dalam ranah siber.

Kata kunci: *Deepfake*, Kejahatan Siber, Regulasi, Literasi Digital

Received: Feb 25, 2025; Revised: Feb 27, 2025; Accepted: Feb 27, 2025; Online Available: March, 2054; Published: April, 2025;
*Corresponding author: *yoan21001@mail.unpad.ac.id*

LATAR BELAKANG

Perkembangan kecerdasan buatan (*artificial intelligence)* telah membawa dampak signifikan dalam berbagai aspek kehidupan, salah satunya adalah dalam bidang rekayasa multimedia. Salah satu teknologi yang berkembang pesat adalah *deepfake*, yang memungkinkan manipulasi konten visual dan audio dengan tingkat realisme yang sangat tinggi. Meskipun memiliki manfaat dalam industri kreatif, *deepfake* juga menghadirkan tantangan baru dalam dunia kejahatan siber (*cybercrime*) seperti ancaman terhadap penipuan identitas, pencemaran nama baik, pemerasan, penyebaran disinformasi, dan manipulasi politik (Haida & Nuriyatman, 2024).

Deepfake adalah teknik yang memanfaatkan AI untuk membuat, menggabungkan, atau memodifikasi gambar, video, atau audio sehingga tampak seperti asli, padahal merupakan hasil rekayasa. Kemampuan *deepfake* untuk meniru wajah dan suara individu dengan sangat meyakinkan telah menimbulkan kekhawatiran terkait penyalahgunaannya dalam berbagai bentuk kejahatan siber, termasuk penipuan, pencemaran nama baik, dan penyebaran informasi palsu (Respati et al., 2024).

Cybercrime adalah segala bentuk pemanfaatan jaringan komputer, sistem informasi, dan teknologi digital untuk melakukan tindakan kriminal yang dapat merugikan individu, kelompok, organisasi, maupun negara (Rifauddin & Halida, 2018). Kejahatan ini mencakup berbagai aktivitas ilegal yang dilakukan dengan menyalahgunakan kemudahan yang ditawarkan oleh perkembangan teknologi informasi dan komunikasi, baik untuk memperoleh keuntungan pribadi, merusak sistem, mencuri data, maupun melakukan sabotase terhadap infrastruktur digital. *Cybercrime* dapat bersifat konvensional, seperti penipuan dan pencurian identitas yang dimodifikasi dalam bentuk digital, maupun bersifat canggih dengan memanfaatkan teknik peretasan, malware, phishing, dan rekayasa sosial untuk menipu atau mengeksploitasi korban. Selain itu, *cybercrime* juga dapat mencakup tindakan yang bertujuan untuk merusak reputasi seseorang, menyebarkan

disinformasi, hingga mengancam keamanan nasional melalui serangan siber yang terorganisir.

Di Indonesia, kasus penyalahgunaan teknologi *deepfake* semakin marak. Salah satu insiden yang mencuri perhatian publik adalah penipuan yang melibatkan penggunaan *deepfake* wajah Presiden Prabowo Subianto. Pelaku menggunakan teknologi ini untuk membuat video palsu yang menampilkan Presiden Prabowo menawarkan bantuan pemerintah, namun dengan syarat korban harus mentransfer sejumlah uang terlebih dahulu. Kasus ini berhasil diungkap oleh Direktorat Tindak Pidana Siber Bareskrim Polri, dengan pelaku berinisial AMA ditangkap di Lampung Tengah pada Januari 2025 (Hukmana, 2025).

Modus operandi yang digunakan dalam kasus tersebut menunjukkan bagaimana teknologi *deepfake* dapat dimanfaatkan untuk menipu masyarakat dengan cara yang semakin canggih. Pelaku tidak hanya menggunakan wajah Presiden Prabowo, tetapi juga Wakil Presiden Gibran Rakabuming Raka dan Menteri Keuangan Sri Mulyani, untuk meyakinkan korban bahwa tawaran bantuan tersebut sah. Akibatnya, lebih dari 100 orang dari 20 provinsi menjadi korban, dengan total kerugian mencapai Rp 65 juta (Meilina, 2025).

Fenomena ini menyoroti urgensi pengaturan hukum yang lebih spesifik terkait penyalahgunaan teknologi *deepfake* di Indonesia. Saat ini, kerangka hukum yang ada belum secara komprehensif mengatur tentang *deepfake*, sehingga penegakan hukum terhadap pelaku seringkali menghadapi kendala. Maka dari itu diperlukan pembaruan dalam undang-undang yang ada atau bahkan pembentukan regulasi baru yang secara khusus mengatur tentang *deepfake* dan implikasinya (Wahyudi, 2025).

Selain aspek hukum, pencegahan kejahatan *deepfake* juga memerlukan pendekatan teknologi. Pengembangan alat deteksi *deepfake* menjadi krusial untuk mengidentifikasi konten yang telah dimanipulasi. Kerja sama antara pemerintah, akademisi, dan sektor swasta diperlukan untuk menciptakan solusi teknologi yang efektif dalam mendeteksi dan mencegah penyebaran konten *deepfake* yang berpotensi merugikan masyarakat.

Pendidikan dan peningkatan kesadaran masyarakat juga memainkan peran penting dalam upaya pencegahan. Masyarakat perlu dibekali dengan pengetahuan tentang apa itu *deepfake*, bagaimana cara kerjanya, serta potensi bahayanya. Dengan demikian, individu dapat lebih waspada dan kritis terhadap konten yang mereka temui di media sosial atau platform digital lainnya, sehingga tidak mudah terperdaya oleh modus penipuan yang memanfaatkan teknologi ini (Respati et al., 2024).

Dalam menghadapi tantangan yang ditimbulkan oleh teknologi *deepfake*, pendekatan multidisipliner yang melibatkan aspek hukum, teknologi, dan edukasi menjadi kunci utama. Hanya dengan kolaborasi dari berbagai pihak, ancaman yang ditimbulkan oleh penyalahgunaan *deepfake* dapat diminimalisir, dan masyarakat dapat terlindungi dari dampak negatifnya.

Penelitian ini bertujuan untuk menganalisis modus kejahatan siber yang memanfaatkan teknologi *deepfake*, khususnya dalam kasus penipuan yang melibatkan manipulasi wajah tokoh publik. Selain itu, penelitian ini juga akan mengevaluasi regulasi yang saat ini berlaku di Indonesia terkait *deepfake* serta mengkaji efektivitas berbagai metode deteksi *deepfake* dalam konteks pencegahan kejahatan siber. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan hukum dan strategi mitigasi kejahatan *deepfake* di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu pendekatan yang berfokus pada norma dan asas hukum dengan mengandalkan sumber-sumber kepustakaan serta peraturan perundang-undangan. Dalam penelitian ini, digunakan berbagai jenis bahan hukum, termasuk bahan hukum primer, seperti peraturan perundang-undangan dan bahan hukum sekunder, seperti buku, jurnal, dan literatur terkait serta bahan hukum tersier, seperti kamus, ensiklopedia, dan sumber referensi lainnya.

Penelitian ini menggunakan metode studi literatur dalam pengumpulan data untuk menganalisis fenomena kejahatan *deepfake* dalam perspektif hukum siber

serta upaya pencegahannya di Indonesia. Studi literatur dilakukan dengan mengumpulkan, mengkaji, dan menganalisis berbagai sumber akademik, termasuk jurnal ilmiah, buku, laporan penelitian, serta regulasi yang berkaitan dengan keamanan siber dan teknologi *deepfake*. Sumber data diperoleh dari berbagai database akademik, seperti Google Scholar, Scopus, serta jurnal nasional terakreditasi, yang membahas aspek hukum, teknologi, dan dampak sosial dari penggunaan *deepfake* dalam konteks kejahatan siber.

HASIL DAN PEMBAHASAN

Peningkatan Kejahatan Siber melalui Teknologi *Deepfake*

Sejalan dengan berjalannya waktu, kecerdasan buatan terus mengalami kemajuan yang signifikan. Hal ini tampak dari semakin banyaknya produk dan layanan yang mengintegrasikan teknologi tersebut. Peningkatan ini sangat menguntungkan karena kecerdasan buatan mampu meningkatkan efisiensi di berbagai bidang. Selain itu, penerapannya memudahkan pelaksanaan berbagai tugas; pekerjaan yang sebelumnya memerlukan keahlian khusus kini dapat dikerjakan oleh siapa saja dengan dukungan teknologi ini. Dengan kemampuan menjalankan algoritma dan model canggih, teknologi ini dapat memahami dan menganalisis data secara cepat dan akurat. Dengan demikian, kecerdasan buatan telah merevolusi cara kita bekerja dan berkomunikasi, mengerjakan tugas-tugas yang dulunya hanya dapat dilakukan oleh manusia.

Namun, di sisi lain, berbagai manfaat dan kemudahan yang dihasilkan oleh penerapan kecerdasan buatan juga berpotensi disalahgunakan untuk tujuan yang merugikan, seperti penggunaan *deepfake* dalam aksi penipuan. Teknologi *deepfake* kini semakin sering dimanfaatkan oleh pelaku kejahatan siber sebagai alat untuk menjalankan aksinya. *Deepfake* memungkinkan pembuatan video atau audio yang tampak autentik, tetapi sebenarnya telah dimanipulasi menggunakan kecerdasan buatan (AI). Kasus penipuan yang melibatkan *deepfake* semakin meningkat, dengan pelaku memanfaatkan teknologi ini untuk menipu korban dengan cara yang lebih meyakinkan. Salah satu contohnya adalah penggunaan wajah tokoh publik untuk menyebarkan informasi palsu demi keuntungan pribadi (H. J. Salim, 2025).

Deepfake memanfaatkan algoritma canggih untuk merekayasa konten dalam bentuk gambar maupun video. Teknologi ini memungkinkan hasil yang dihasilkan memiliki tingkat akurasi dan kemiripan yang sangat tinggi. Dalam pengembangannya, *deepfake* menggunakan algoritma *deep learning*, salah satu model *machine learning* yang sering diterapkan adalah *Generative Adversarial Networks* (GANs). GANs terdiri dari dua komponen utama, yaitu *generator* dan *discriminator*, yang masing-masing memiliki peran berbeda. *Generator* berperan dalam menghasilkan data baru yang mirip dengan data asli, sementara *discriminator* bertugas membedakan antara data asli dan data yang dibuat oleh *generator.* Kedua komponen ini bekerja secara bersaing dalam proses pembelajaran dimana *generator* terus belajar untuk menghasilkan data yang semakin mirip dengan data asli, sementara discriminator semakin terlatih dalam membedakan antara data asli dan data buatan (M. P. Salim, 2024).

Kasus penipuan yang melibatkan *deepfake* dengan wajah Presiden Prabowo Subianto menjadi sorotan utama dalam diskusi mengenai ancaman teknologi kecerdasan buatan dalam kejahatan siber. Pelaku menggunakan teknologi AI untuk menciptakan video yang menampilkan wajah dan suara yang sangat mirip dengan Presiden Prabowo, seolah-olah ia secara langsung menawarkan bantuan keuangan kepada masyarakat. Video tersebut kemudian dibagikan melalui platform media sosial, menarik perhatian banyak orang yang menganggap tawaran tersebut sebagai sesuatu yang autentik. Kecepatan penyebaran dan tingkat kemiripan video *deepfake* ini menunjukkan betapa efektifnya teknologi ini dalam mengecoh publik.

Modus operandi ini mengungkapkan tantangan besar dalam mendeteksi dan menangkal penyalahgunaan *deepfake* di era digital. Kasus ini menyoroti urgensi regulasi dan mekanisme verifikasi yang lebih ketat untuk memastikan keaslian konten digital, terutama yang melibatkan figur publik. Selain itu, perlu adanya kerja sama antara pemerintah, penyedia platform media sosial, serta masyarakat dalam meningkatkan literasi digital guna mencegah dampak negatif dari penyebaran informasi palsu berbasis *deepfake*.

Selain Presiden Prabowo, pelaku juga memanfaatkan wajah Wakil Presiden Gibran Rakabuming Raka dan Menteri Keuangan Sri Mulyani dalam video penipuan mereka. Hal ini menunjukkan bahwa pelaku tidak ragu untuk menggunakan identitas pejabat tinggi negara untuk mencapai tujuan mereka. Dengan memanfaatkan teknologi *deepfake*, pelaku dapat menciptakan konten yang tampak autentik, sehingga korban lebih mudah terperdaya. Kasus ini menekankan pentingnya kewaspadaan masyarakat terhadap informasi yang diterima, terutama yang berasal dari sumber yang tidak resmi (Octavia & Prabowo, 2025).

Dampak dari penipuan ini cukup signifikan, baik dari segi finansial maupun sosial. Banyak korban yang tertipu dan mentransfer sejumlah uang dengan harapan mendapatkan bantuan yang dijanjikan. Menurut laporan, pelaku berhasil mengumpulkan puluhan juta rupiah dari korban-korbannya dalam kurun waktu beberapa bulan. Kerugian finansial ini menunjukkan bagaimana teknologi *deepfake* dapat dimanfaatkan untuk mengeksploitasi kepercayaan masyarakat, terutama dalam situasi yang melibatkan tokoh publik dan janji bantuan keuangan.

Selain kerugian material, dampak psikologis dan sosial juga menjadi konsekuensi serius dari tindakan penipuan semacam ini. Banyak korban yang mengalami tekanan emosional akibat merasa tertipu, sementara kepercayaan masyarakat terhadap informasi resmi turut terguncang. Masyarakat menjadi lebih skeptis terhadap komunikasi dari pemerintah atau lembaga resmi, yang pada akhirnya dapat menghambat efektivitas penyampaian informasi penting. Oleh karena itu, diperlukan langkah-langkah pencegahan yang lebih ketat, termasuk peningkatan kesadaran publik mengenai *deepfake* serta penguatan regulasi untuk menanggulangi penyalahgunaan teknologi ini.

Kasus ini juga mengungkap tantangan yang dihadapi oleh aparat penegak hukum dalam menangani kejahatan siber yang memanfaatkan teknologi canggih seperti *deepfake*. Diperlukan alat dan metode yang lebih maju untuk mendeteksi dan mencegah penyebaran konten *deepfake.* Selain itu, kerjasama antara pemerintah, penegak hukum, dan platform media sosial menjadi krusial dalam upaya memerangi penyalahgunaan teknologi ini. Edukasi kepada masyarakat tentang bahaya dan cara

mengenali *deepfake* juga menjadi langkah penting dalam pencegahan kejahatan siber di era digital ini.

Peran Edukasi Masyarakat dalam Pencegahan Penipuan *Deepfake*

Edukasi masyarakat memegang peranan kunci dalam mencegah penipuan yang memanfaatkan teknologi *deepfake*. Dengan pemahaman yang baik mengenai cara kerja dan ciri-ciri konten *deepfake*, masyarakat dapat lebih waspada dan kritis terhadap informasi yang diterima. Salah satu langkah penting adalah meningkatkan literasi digital, sehingga individu mampu mengenali tanda-tanda manipulasi dalam konten multimedia (Fauzi et al., 2023).

Pemerintah dan lembaga terkait perlu menginisiasi program sosialisasi yang menyasar berbagai lapisan masyarakat. Program ini dapat berupa seminar, *workshop*, atau kampanye melalui media sosial yang menjelaskan bahaya *deepfake* dan cara mengidentifikasinya. Dengan demikian, masyarakat akan lebih siap menghadapi ancaman penipuan yang semakin canggih dan tidak mudah terperdaya oleh konten palsu yang beredar (Jufri & Putra, 2021).

Selain itu, kolaborasi antara sektor pendidikan dan teknologi juga penting dalam upaya pencegahan kejahatan *deepfake*. Inklusi materi mengenai keamanan digital dan deteksi *deepfake* dalam kurikulum pendidikan dapat membekali generasi muda dengan keterampilan yang diperlukan untuk menghadapi tantangan di era digital. Pendidikan mengenai cara kerja teknologi kecerdasan buatan yang digunakan dalam *deepfake*, serta strategi untuk mengenali manipulasi digital, dapat meningkatkan kesadaran dan kewaspadaan masyarakat. Dengan demikian, individu tidak hanya menjadi pengguna teknologi, tetapi juga memiliki pemahaman kritis terhadap potensi penyalahgunaannya.

Pendekatan ini memastikan bahwa kesadaran akan ancaman *deepfake* ditanamkan sejak dini, membentuk masyarakat yang lebih tangguh terhadap penipuan digital. Selain melalui pendidikan formal, pelatihan literasi digital bagi masyarakat luas juga diperlukan, termasuk kampanye kesadaran publik yang melibatkan media sosial, komunitas, dan sektor swasta. Kerja sama antara pemerintah, institusi pendidikan, serta perusahaan teknologi dalam menyediakan

sumber daya dan alat pendeteksi *deepfake*dapat memperkuat ekosistem keamanan digital. Dengan upaya yang terkoordinasi dan berkelanjutan, risiko penyebaran konten manipulatif berbasis *deepfake* dapat ditekan, sehingga masyarakat lebih terlindungi dari dampak negatif kejahatan siber.

Platform media sosial dan perusahaan teknologi juga memiliki tanggung jawab dalam mengedukasi pengguna mereka. Dengan menyediakan alat dan sumber daya yang membantu pengguna mengenali dan melaporkan konten *deepfake*, platform dapat berkontribusi dalam mengurangi penyebaran informasi palsu. Langkah proaktif ini tidak hanya melindungi pengguna, tetapi juga menjaga integritas ekosistem digital secara keseluruhan (Banfatin et al., 2024).

Terakhir, penting bagi individu untuk selalu memverifikasi informasi sebelum mempercayainya atau membagikannya kepada orang lain. Sikap kritis dan kehati-hatian dalam menerima informasi, terutama yang berasal dari sumber yang tidak jelas, dapat mencegah penyebaran penipuan berbasis *deepfake*. Edukasi mengenai metode verifikasi, seperti pengecekan sumber, analisis metadata, dan penggunaan alat pendeteksi *deepfake*, menjadi langkah esensial dalam membangun kesadaran digital di masyarakat.

Dengan membudayakan kebiasaan cek fakta, masyarakat dapat secara kolektif meminimalkan dampak negatif dari teknologi *deepfake*. Kesadaran ini juga perlu didukung oleh platform digital yang lebih bertanggung jawab dalam menyaring dan menandai konten manipulatif. Regulasi yang jelas serta penguatan etika dalam penggunaan kecerdasan buatan juga berperan dalam mengurangi risiko penyalahgunaan teknologi ini. Dengan kombinasi literasi digital, pengawasan yang ketat, dan teknologi pendukung, potensi bahaya *deepfake* dapat dikendalikan, sehingga ruang digital menjadi lebih aman dan terpercaya

Urgensi Pengaturan Hukum terhadap Teknologi *Deepfake* di Indonesia

Teknologi *deepfake*, yang memungkinkan pembuatan konten palsu menggunakan kecerdasan buatan (AI), telah menjadi ancaman serius di berbagai bidang, termasuk keamanan siber, privasi, dan kepercayaan publik. Kasus penipuan *deepfake* yang melibatkan wajah Presiden Prabowo Subianto menjadi contoh nyata

betapa teknologi ini dapat disalahgunakan untuk menipu masyarakat dan merusak reputasi individu. Meskipun pelaku dalam kasus ini telah dijerat dengan Pasal 51 ayat (1) jo Pasal 35 UU ITE dan Pasal 378 KUHP, kasus ini mengungkapkan kelemahan regulasi yang ada dan mendorong perlunya pengaturan hukum yang lebih spesifik dan komprehensif.

Dalam kasus ini, pelaku menggunakan teknologi *deepfake* untuk memanipulasi wajah Presiden Prabowo Subianto dalam sebuah video yang disebarkan secara online. Video tersebut digunakan untuk menipu masyarakat dengan menyampaikan pesan palsu yang seolah-olah berasal dari Presiden. Pelaku memanfaatkan kecanggihan teknologi *deepfake* untuk membuat konten yang terlihat sangat nyata, sehingga sulit dibedakan dari konten asli.

Pelaku dalam kasus ini dijerat dengan dua pasal utama yaitu Pasal 51 ayat (1) jo Pasal 35 UU ITE dan Pasal 378 Kitab Undang-Undang Hukum Pidana. Pasal 51 ayat (1) jo Pasal 35 UU ITE mengatur tentang manipulasi informasi elektronik yang dapat merugikan orang lain atau masyarakat. Pelaku dianggap telah memanipulasi informasi elektronik dengan sengaja untuk menipu. Sementara itu, Pasal 378 Kitab Undang-Undang Hukum Pidana mengatur tentang tindak pidana penipuan, yang mencakup upaya untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan cara menipu. Pada pasal-pasal ini dijelaskan bahwa ancaman hukuman bagi pelaku adalah penjara antara 4 hingga 12 tahun dan denda maksimal Rp12 miliar. Penerapan pasal-pasal ini menunjukkan komitmen pemerintah dalam menindak tegas kejahatan siber yang memanfaatkan teknologi canggih.

Meskipun beberapa pasal dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) dapat digunakan untuk menangani kasus *deepfake,* terdapat beberapa kelemahan yang membuat regulasi ini kurang efektif dalam memberikan perlindungan hukum yang komprehensif. Salah satu kelemahan utama adalah ketidaksesuaian regulasi yang ada dengan perkembangan teknologi. UU ITE dan KUHP tidak secara spesifik mengatur tentang *deepfak*e, sehingga penerapannya masih bersifat umum dan kurang tepat sasaran dalam menangani kasus-kasus yang berkaitan dengan

manipulasi digital berbasis kecerdasan buatan. Selain itu, terdapat tantangan besar dalam proses identifikasi dan pembuktian di ranah hukum. Teknologi *deepfake* yang semakin canggih membuat konten palsu sulit dibedakan dari yang asli, sehingga menyulitkan aparat penegak hukum dalam mengumpulkan bukti yang valid dan membuktikan niat jahat pelaku. Kurangnya pemahaman dan kesiapan teknis dalam mengatasi kejahatan berbasis AI ini juga semakin memperumit proses penegakan hukum. Selain itu, regulasi yang ada masih memiliki keterbatasan dalam perlindungan terhadap korban, baik dari segi psikologis, sosial, maupun pemulihan reputasi. Saat ini, belum tersedia mekanisme yang efektif untuk menangani dampak negatif yang ditimbulkan oleh *deepfake* terhadap individu yang menjadi korban, termasuk akses terhadap bantuan hukum, pemulihan nama baik, serta upaya untuk menghapus atau mengendalikan penyebaran konten yang merugikan.

Indonesia membutuhkan peraturan hukum yang spesifik dalam mengatur *Artificial Intelligence* (AI) guna menjamin penggunaan teknologi ini tetap berada dalam koridor hukum yang etis, bertanggung jawab, serta melindungi kepentingan masyarakat dan negara. Hal ini sejalan dengan pandangan Mochtar Kusumaatmadja yang menegaskan bahwa perubahan terhadap hukum dapat terjadi melalui pembentukan hukum positif yang harus disesuaikan dengan nilai dan fakta yang berkembang di masyarakat (Setiarma, 2023). Oleh karena itu, diperlukan Undang-Undang *Artificial Intelligence* (*Law of Artificial Intelligence*) yang secara khusus mengatur berbagai aspek penggunaan AI, termasuk pengiriman dan penerimaan pesan elektronik melalui teknologi AI, pemanfaatan AI dalam sektor ekonomi dan pemerintahan, serta mitigasi terhadap risiko penyalahgunaan AI yang dapat merugikan individu maupun kepentingan publik (Patikasari, 2024).

Deepfake memiliki potensi besar untuk disalahgunakan dalam berbagai aspek kehidupan, termasuk dalam penipuan, pencemaran nama baik, disinformasi politik, eksploitasi seksual digital, hingga serangan siber yang dapat mengancam keamanan nasional. Oleh karena itu, regulasi baru harus memberikan definisi yang jelas tentang *deepfake*, termasuk batasan antara penggunaan yang sah (seperti dalam industri hiburan, seni, atau pendidikan) dan penyalahgunaan yang dapat menimbulkan dampak negatif bagi individu maupun masyarakat luas.

Dalam konteks keamanan siber, Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber (RUU KKS) memiliki peran penting dalam membangun sistem pertahanan siber nasional yang kuat terhadap ancaman teknologi *deepfake*. RUU KKS dirancang untuk meningkatkan kapasitas negara dalam menangkal serangan siber dan penyebaran informasi palsu yang dapat mengganggu stabilitas sosial, politik, dan ekonomi. Hal ini mengingat *deepfake* telah banyak digunakan dalam kampanye disinformasi politik, baik di dalam maupun luar negeri, urgensi regulasi ini semakin meningkat, terutama menjelang pemilu dan peristiwa politik penting lainnya. RUU KKS perlu memasukkan ketentuan yang mengatur pencegahan dan penindakan terhadap penyalahgunaan *deepfake*, termasuk melalui kerja sama dengan platform digital dalam mendeteksi dan menghapus konten yang terbukti merugikan masyarakat.

Pemerintah perlu bekerja sama dengan ahli teknologi, akademisi, serta sektor industri dalam mengembangkan alat deteksi *deepfake* yang dapat digunakan oleh aparat penegak hukum dan masyarakat umum (Fadillah et al., 2025). Regulasi harus memastikan bahwa alat ini dapat diakses secara luas, memiliki tingkat akurasi tinggi, serta dapat membedakan konten *deepfake* yang berbahaya dari manipulasi digital yang sah. Selain itu, RUU KKS harus memberikan pedoman bagi institusi pemerintah dalam menangani ancaman *deepfake*, termasuk dengan membentuk pusat deteksi *deepfake* nasional yang bertugas mengawasi dan menanggulangi penyebaran konten *deepfake* yang berpotensi membahayakan kepentingan nasional.

Dari aspek penegakan hukum, regulasi juga harus mengatur sanksi yang tegas dan proporsional bagi pelaku yang menyalahgunakan teknologi *deepfake* untuk tujuan kriminal. Dalam kasus penipuan berbasis *deepfake*, di mana seseorang menciptakan identitas palsu untuk melakukan tindak pidana, hukuman pidana harus diterapkan secara tegas. Selain hukuman penjara, pelaku juga harus dikenakan denda dalam jumlah besar, serta diwajibkan untuk memulihkan reputasi korban. Penggunaan *deepfake* untuk tujuan eksploitasi seksual digital, seperti pembuatan konten pornografi tanpa izin korban, juga harus dikategorikan sebagai

kejahatan serius, dengan hukuman yang setimpal dengan dampak psikologis dan sosial yang ditimbulkan.

Selain menghukum pelaku, RUU KKS juga dapat memperkenalkan mekanisme sanksi administratif bagi platform digital yang gagal dalam menangani penyebaran *deepfake* yang berbahaya. Platform media sosial dan layanan berbasis AI harus memiliki sistem pendeteksian otomatis yang dapat mengidentifikasi dan menandai konten *deepfake* yang berpotensi merugikan publik. Jika sebuah platform tidak memiliki kebijakan moderasi yang memadai, maka pemerintah dapat menjatuhkan sanksi berupa denda, pembatasan akses, atau bahkan pencabutan izin operasional jika terbukti membiarkan penyebaran *deepfake* yang merugikan masyarakat.

Selain aspek penindakan, regulasi juga harus mencakup mekanisme perlindungan bagi korban *deepfake*, termasuk bantuan hukum, dukungan psikologis, serta upaya pemulihan reputasi. Korban *deepfake* harus diberikan hak untuk menuntut ganti rugi, baik dari pelaku maupun dari platform yang gagal mengambil tindakan terhadap penyebaran konten yang merugikan. Dalam konteks ini, RUU KKS dan UU AI harus bekerja secara sinergis, di mana RUU KKS berfokus pada penguatan keamanan siber dan penegakan hukum terhadap serangan digital, sementara UU tentang AI harus mengatur standar etika dan transparansi dalam pengembangan teknologi AI, termasuk dalam aspek tanggung jawab pengembang terhadap dampak sosial dari teknologi yang mereka ciptakan.

Pada berbagai negara, regulasi tentang AI mulai berkembang pesat untuk mengantisipasi dampak teknologi ini terhadap masyarakat. Uni Eropa telah mengeluarkan proposal regulasi AI yang menetapkan kategori risiko dalam penggunaan AI, di mana *deepfake* termasuk dalam kategori yang membutuhkan pengawasan ketat. Amerika Serikat juga mulai menerapkan kebijakan transparansi bagi perusahaan teknologi yang menggunakan AI dalam pembuatan konten digital. Indonesia perlu mengikuti langkah serupa dengan membentuk UU tentang AI yang dapat memberikan pedoman komprehensif dalam penggunaan teknologi AI, termasuk dalam hal akuntabilitas pengembang, transparansi algoritma, serta mekanisme audit terhadap sistem AI yang digunakan di sektor publik dan swasta.

Tanpa regulasi yang memadai, Indonesia berisiko menjadi negara konsumen teknologi AI tanpa memiliki perlindungan hukum yang cukup terhadap dampak negatifnya. Oleh karena itu, RUU KKS dan UU tentang AI harus segera dirumuskan dan disahkan untuk menciptakan lingkungan digital yang lebih aman, inovatif, serta sesuai dengan prinsip-prinsip hukum dan etika yang berlaku. Dengan pendekatan yang tepat, Indonesia dapat memanfaatkan teknologi AI untuk kemajuan bangsa, sekaligus melindungi masyarakat dari ancaman yang ditimbulkan oleh penyalahgunaan teknologi ini

KESIMPULAN DAN SARAN

Teknologi *deepfake* telah menjadi ancaman serius dalam kejahatan siber, memungkinkan pelaku untuk menipu masyarakat melalui manipulasi video dan audio yang sangat meyakinkan. Kasus penipuan yang melibatkan tokoh publik, seperti Presiden Prabowo Subianto dan pejabat lainnya, menunjukkan bagaimana *deepfake* dapat digunakan untuk menyebarkan informasi palsu dan merugikan korban secara finansial maupun psikologis. Tantangan utama dalam menghadapi kejahatan ini adalah meningkatnya kompleksitas teknologi yang menyulitkan deteksi serta penegakan hukum yang efektif.

Oleh karena itu, dalam rangka mengatasi ancaman ini, diperlukan regulasi yang lebih spesifik terkait penggunaan *deepfake*, serta peningkatan literasi digital di masyarakat. Pemerintah, platform media sosial, dan lembaga penegak hukum harus bekerja sama dalam mendeteksi, mencegah, dan menangani penyebaran konten *deepfake* yang berbahaya. Selain itu, edukasi publik tentang cara mengenali *deepfake* menjadi langkah penting dalam meminimalkan dampak negatifnya, sehingga masyarakat dapat lebih kritis dan tidak mudah terperdaya oleh informasi palsu.

DAFTAR REFERENSI

Banfatin, P. M., Medan, K. K., & Fallo, D. F. N. (2024). Pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi artificial intelligence deepfake dalam melakukan tindak pidana cybercrime. *Pemuliaan Keadilan*, *2*(1), 60–73. https://doi.org/10.62383/pk.v2i1.402

Fadillah, M. F., Nazar, & Setiawan, H. (2025). Dampak teknologi deepfake terhadap

kepercayaan publik dan penyebaran informasi di media sosial. *ResearchGate*.

Fauzi, A. M., Wahyuni, A. T., Chintia, G., Nenci, I. S., Nurwahidah, N., & Sari, P. N. (2023). Edukasi pencegahan penipuan online berbasis sosial media di Desa Mekarwangi. *Jurnal Pengabdian Kepada Masyarakat*, *3*(2), 60–73.

Haida, R. S. N., & Nuriyatman, E. (2024). Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence (AI) Dari Perspektif Hukum Pidana Indonesia. *Jurnal Hukum Respublica*, *24*(1), 2–3.

Hukmana, S. Y. (2025). Penipuan dengan AI deepfake wajah Prabowo, warga tertipu tawaran bantuan pemerintah. *Media Indonesia*. Diakses pada 21 Februari 2025. https://mediaindonesia.com/politik-dan-hukum/741824/penipuan-dengan-ai-deepfake-wajah-prabowo-warga-tertipu-tawaran-bantuan-pemerintah?

Jufri, M. A. A., & Putra, A. K. (2021). Aspek hukum internasional dalam pemanfaatan deepfake technology terhadap perlindungan data pribadi. *Uti Possidetis: Journal of International Law*, *1*(31–57).

Meilina, K. (2025). Penipuan bansos pakai AI wajah Prabowo, ratusan korban rugi puluhan juta. *Katadata.Co.Id*. Diakses pada 21 Februari 2025. https://katadata.co.id/digital/teknologi/67a5dc910647b/penipuan-bansos-pakai-ai-wajah-prabowo-ratusan-korban-rugi-puluhan-juta?

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi deepfake di Indonesia sebagai bentuk pelindungan negara. *Jurnal USM Law Review*, *7*(2).

Octavia, S., & Prabowo, D. (2025). Wajah hingga suara Gibran dan Sri Mulyani ikut dicatut untuk tipu korban via video "deepfake." *Kompas.Com*. Diakses pada 22 Februari 2025. https://nasional.kompas.com/read/2025/01/23/21051441/wajah-hingga-suara-gibran-dan-sri-mulyani-ikut-dicatut-untuk-tipu-korban-via

Patikasari, T. (2024). *Pelindungan hukum bagi korban deepfake pornografi (studi perbandingan Indonesia dan Korea Selatan)*. UIN Syarif Hidayatullah Jakarta.

Pengaturan hukum teknologi deepfake di Indonesia. (2024). ALO Alchemist Group. https://alchemistgroup.co/pengaturan-hukum-teknologi-deepfake-di-indonesia/?

Respati, A. A., Setyarini, A. D., Parlagutan, D., Rafli, M., Mahendra, R. S., & Nugroho, A. A. (2024). Analisis hukum terhadap pencegahan kasus deepfake serta perlindungan hukum terhadap korban. *Media Hukum Indonesia (MHI)*, *2*(2), 586. https://doi.org/10.5281/zenodo.12508126

Rifauddin, M., & Halida, A. N. (2018). Waspada cybercrime dan informasi hoax pada media sosial facebook. *Khizanah Al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, *6*(2).

Salim, H. J. (2025). Pelaku penipuan deepfake AI Prabowo ditangkap, begini modus kejahatannya. *Liputan6.Com*. Diakses pada 22 Februari 2025. https://www.liputan6.com/cek-fakta/read/5894584/pelaku-penipuan-deepfake-ai-prabowo-ditangkap-begini-modus-kejahatannya?

Salim, M. P. (2024). Apa Itu Deepfake? Pahami Cara Kerja,Kontroversi Penyalahgunaannya, Serta Regulasi Penggunaannya. *Liputan6.Com*. https://www.liputan6.com/hot/read/5497453/apa-itu-deepfake-pahami-cara-kerja-kontroversi-penyalahgunaannya-serta-regulasi-penggunaannya?page=7

Setiarma, A. (2023). Disrupsi Teknologi Hukum Terhadap Jasa Advokat Dalam Pandangan Hukum Pembangunan Mochtar Kusumaatmadja: The Disruption of Legal Technology to the Advocates Services in the Perspective of Mochtar Kusumaatmadja's Legal Development. *Reformasi Hukum*, *27*(2), 88.

Wahyudi, B. R. (2025). Tantangan penegakan hukum terhadap kejahatan berbasis teknologi AI. *Innovative: Journal of Social Science Research*, *5*(1), 3436–3450. https://doi.org/10.31004/innovative.v5i1.17519