YURIJAYA, Jurnal Ilmiah Hukum
Pengkajian Masalah Hukum dan Pembangunan – Vol. 7 No. 3 (2025) : Desember
e-ISSN : 2581-0243 p-ISSN : 2087-3409

DEEP FAKE CRIME ON SOCIAL MEDIA: A JURIDICAL ANALYSIS OF THE SPREAD OF HOAXES AND THE MANIPULATION OF PUBLIC OPINION IN STATE SECURITY

Firdausi Nur Fa'izah, Universitas Negeri Surabaya; 25131585023@mhs.unesa.ac.id
Roihatul Jannah Kurniasari, Universitas Negeri Surabaya; 25131585011@mhs.unesa.ac.id

Abstrak: Perkembangan kecerdasan buatan (*Artificial Intelligence*/AI) telah membawa dampak besar terhadap pola komunikasi dan penyebaran informasi di media sosial. Di balik manfaatnya, teknologi ini juga menimbulkan ancaman baru berupa penyebaran hoaks dan manipulasi opini publik, terutama pada masa demonstrasi ketika masyarakat sangat bergantung pada informasi digital. Penggunaan *deepfake*, *AI bot*, dan konten otomatis sering dimanfaatkan untuk menciptakan narasi palsu yang dapat memicu keresahan sosial. Kondisi ini menunjukkan bahwa hukum positif di Indonesia, khususnya UU ITE, belum sepenuhnya mampu menjangkau karakteristik kejahatan berbasis AI yang kompleks dan sulit dibuktikan. Penulis ini menganalisis bentuk dan modus operandi kejahatan AI di media sosial serta mengkaji tanggung jawab hukum pelaku, pengembang, dan platform yang terlibat. Menimbulkan dapak pada Penyalahgunaan atau manipulasi deep fake tidak hanya ditujukan untuk hiburan atau untuk mencemarkan reputasi seseorang, tetapi dalam skala besar juga digunakan untuk membentuk opini publik, mengalihkan isu hingga propaganda. Melalui menyebarkan berita hoax dan cybercrime untuk memicu cyberterrorism. Keberadaannya dalam cyberterrorism yang terus semakin berkembang. Penelitian hukum ini membahas manipulasi data pribadi ke dalam teknologi deep fake dan dampaknya terhadap cyberterrorism, ketahanan politik dan hukum di Indonesia. Serta menggunakan teori cross-border crime (kejahatan lintas batas negara). Teori ini menjelaskan bahwa kejahatan modern, khususnya kejahatan siber, tidak lagi terikat oleh batas geografis suatu negara. Pelaku kejahatan deep fake dapat beroperasi dari negara lain dengan target negara yang berbeda. Hasil kajian menegaskan perlunya pembaruan regulasi, peningkatan kapasitas penegakan hukum, dan kerja sama lintas sektor untuk menanggulangi penyalahgunaan AI di ruang digital dalam memeperkuat keamana negara.
Kata kunci: *Artificial Intelligence; Deep Fake; Cybercrime; Cyberterrorism; Cybersecurity*

Abstract: The development of artificial intelligence (AI) has had a major impact on communication patterns and the dissemination of information on social media. Behind its benefits, this technology also poses a new threat in the form of the spread of hoaxes and manipulation of public opinion, especially during demonstrations when people are heavily dependent on digital information. The use of deepfakes, AI bots, and automated content is often used to create false narratives that can trigger social unrest. This condition shows that positive law in Indonesia, especially the ITE Law, has not been fully able to reach the characteristics of AI-based crimes that are complex and difficult to prove. This author analyzes the forms and modus operandi of AI crimes on social media and examines the legal responsibilities of the perpetrators, developers, and platforms involved. Causing a footprint on the abuse or manipulation of deep fakes is not only intended for entertainment or to defame a person, but on a large scale is also used to shape public opinion, diverting issues to propaganda. Through spreading hoax news and cybercrime to trigger cyberterrorism. Its existence in cyberterrorism

continues to grow. This legal research discusses the manipulation of personal data into deep fake technology and its impact on cyberterrorism, political and legal resilience in Indonesia. As well as using the theory of cross-border crime. This theory explains that modern crime, particularly cybercrime, is no longer bound by the geographical boundaries of a country. Deep fake criminals can operate from other countries with different country targets. The results of the study emphasized the need for regulatory reform, law enforcement capacity building, and cross-sector cooperation to overcome the abuse of AI in the digital space in strengthening state security.
Keywords: *Artificial Intelligence; Deep Fake; Cybercrime; Cyberterrorism; Cybersecurity*

PENDAHULUAN

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) telah memberikan pengaruh besar terhadap kehidupan sosial, ekonomi, dan politik di era digital. AI kini tidak hanya menjadi alat bantu manusia dalam mempermudah pekerjaan, tetapi juga berperan aktif dalam memproduksi dan menyebarkan informasi melalui algoritma yang kompleks. Di bidang komunikasi massa, teknologi AI mampu mengelola data dalam jumlah besar untuk menentukan preferensi pengguna dan mengarahkan arus informasi sesuai dengan pola perilaku mereka. Hal ini menciptakan sistem media sosial yang sangat dinamis, namun sekaligus rentan terhadap penyalahgunaan. Di tengah keterbukaan informasi yang tidak terbatas, muncul persoalan baru berupa penyebaran hoaks dan manipulasi opini publik yang memanfaatkan kecanggihan teknologi AI.

Media sosial, yang pada awalnya dirancang sebagai sarana komunikasi dan berbagi informasi, kini menjadi arena utama dalam penyebaran informasi yang tidak selalu dapat diverifikasi kebenarannya. Penggunaan AI untuk memproduksi konten palsu seperti *deepfake videos*, gambar sintetis, atau teks yang dihasilkan oleh mesin, telah memperburuk masalah disinformasi. Teknologi *chatbot* dan *automated bot* memungkinkan penyebaran pesan palsu dalam skala masif, menciptakan kesan bahwa suatu opini didukung banyak pihak padahal hanya hasil manipulasi sistem. Fenomena ini sering kali digunakan oleh pihak-pihak tertentu untuk menggiring opini publik demi kepentingan politik atau ekonomi. Akibatnya, ruang publik digital menjadi semakin sulit dibedakan antara kebenaran dan kepalsuan. Maka menimbukan peluang untuk menggunakan teknologi informasi untuk tujuan destruktif berkaitan dengan masyarakat dan kebijakan hukum ketika digunakan oleh penjahat siber untuk kegiatan seperti cyberbullying dan cyberterrorism, yang harus diperhitungkan.

Teori *cross border crime* (kejahatan lintas batas negara**)** menjelaskan bahwa perkembangan globalisasi dan teknologi digital telah menghilangkan batas teritorial dalam kejahatan. Pelaku dapat melakukan tindak kejahatan dari satu negara dengan dampak yang dirasakan di negara lain. Kondisi ini menyulitkan penegakan hukum

karena adanya perbedaan yurisdiksi, sistem hukum, dan kepentingan antarnegara. Oleh karena itu, kejahatan lintas batas dipandang sebagai ancaman serius terhadap keamanan nasional dan internasional. Dalam perspektif teori ini, teknologi digital berperan besar dalam mempercepat dan mempermudah terjadinya kejahatan lintas negara. Internet memungkinkan pelaku beroperasi secara anonim, cepat, dan masif tanpa harus berada di wilayah negara target. Negara sering mengalami keterbatasan dalam pelacakan pelaku dan pengumpulan bukti hukum. Hal ini menunjukkan bahwa hukum nasional saja tidak cukup untuk menangani kejahatan lintas batas.

Kejahatan AI berupa *deepfake* merupakan bentuk nyata dari cross-border crime. Pelaku deep fake dapat menciptakan dan menyebarkan konten palsu dari luar negeri untuk mengganggu stabilitas politik, sosial, dan keamanan negara lain. Kejahatan ini sulit dikendalikan oleh satu negara karena sifatnya yang lintas batas dan berbasis teknologi global. Dengan demikian, penanggulangan deep fake memerlukan kerja sama internasional, harmonisasi regulasi, dan penguatan keamanan siber sebagai bagian dari strategi menghadapi kejahatan lintas negara.

Situasi ini menjadi sangat berbahaya ketika terjadi pada momen sosial dan politik yang sensitif, seperti saat berlangsungnya demonstrasi atau aksi massa. Pada kondisi tersebut, masyarakat sangat bergantung pada arus informasi dari media sosial untuk mengetahui situasi terkini di lapangan. Ketika AI digunakan untuk menyebarkan hoaks atau mengubah persepsi publik terhadap suatu peristiwa, dampaknya dapat memicu keresahan, provokasi, bahkan tindakan anarkis. Penyebaran konten palsu yang menyerupai fakta lapangan menyebabkan masyarakat mudah terprovokasi dan kehilangan kemampuan untuk menilai kebenaran informasi. Dengan demikian, kejahatan AI di media sosial tidak hanya berdampak pada individu, tetapi juga berpotensi mengganggu stabilitas sosial dan keamanan nasional.

Fenomena penyalahgunaan AI ini menunjukkan adanya tantangan baru dalam penegakan hukum di Indonesia. Regulasi yang ada, terutama Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, memang telah memberikan dasar hukum dalam menangani kejahatan siber. Namun, ketentuan tersebut belum secara spesifik mengatur bentuk-bentuk kejahatan yang muncul akibat perkembangan teknologi AI. Sifat AI yang otonom dan kompleks menjadikan penentuan pelaku, motif, serta tanggung jawab hukumnya sulit dilakukan. Selain itu, aspek teknis seperti pembuktian digital, otentikasi konten, dan identifikasi sumber penyebar informasi menjadi kendala serius dalam proses penegakan hukum.

Di sisi lain, tanggung jawab tidak hanya terletak pada individu yang menyebarkan konten palsu, tetapi juga pada pengembang sistem AI dan platform media sosial tempat konten tersebut beredar. Platform sering kali berperan ganda,

yaitu sebagai penyedia teknologi dan sekaligus pengendali arus informasi publik. Namun, sejauh mana tanggung jawab hukum dapat dibebankan kepada mereka masih menjadi perdebatan. Dalam konteks hukum Indonesia, belum ada aturan tegas yang mengatur kewajiban platform untuk mengawasi konten berbasis AI secara preventif. Hal ini menunjukkan adanya kekosongan hukum yang perlu segera diisi untuk memberikan kepastian dan perlindungan hukum bagi masyarakat pengguna media sosial.

Kejahatan AI di media sosial juga harus dipandang sebagai fenomena multidimensional yang tidak hanya menyangkut aspek teknologi dan hukum, tetapi juga etika dan sosial. Pemanfaatan AI yang mana memiliki kecanggihan pengenalan wajah dan suara dengan bantuan kecerdasan buatan (artificial intelligence) sehingga karakteristik penentu wajah dan suara manusia sebagai pengenal unik mereka akan disimpan dalam basis data sistem penyedia layanan tanpa pengawasan etis dapat melanggar hak privasi, menciptakan ketidakadilan informasi, dan memperlemah kepercayaan publik terhadap sumber berita resmi. Oleh karena itu, pendekatan yuridis perlu dikombinasikan dengan penguatan literasi digital dan kesadaran hukum masyarakat. Masyarakat perlu memahami risiko dari interaksi dengan konten digital yang dihasilkan oleh AI, sehingga tidak mudah terpengaruh atau ikut serta dalam penyebaran hoaks yang merugikan banyak pihak.

Terdapat beberapa penelitian terdahulu yang membahas mengenai topik terkait kajian ini yaitu yang pertama adalah penelitian yang berjudul Perlindungan Hukum Terhadap *Artificial Intellegence* Dalam Aspek Penyalahgunaan *Deepfake Technology* Pada Perspektif UU PDP Dan GDPR oleh Jeremiah Maximillian Laza dan Rizky Karo Karo, yang membedakan penelitian tersebut dengan kajian ini adalah penelitian tersebut hanya berfokus pada deepfake ditinjau dari UU PDP dan GDPR saja [1]. Kemudian penelitian yang mebahas topik serupa lainnya yakni penelitian berjudul Penggunaan *Deepfake* Terkait Penyebaran Isu Hoaks Pada Masa Kampanye Pemilu 2024 oleh Wilma Silalahi, Meily Natassya, dan Shane Evelina, untuk penelitian tersebut hanya berfokus pada penggunaan *deepfake* untuk menyebarkan hoaks pada saat kampanye pemilu 2024 saja [2].

Berdasarkan kondisi tersebut, penulis memandang penting untuk melakukan kajian yang mendalam mengenai kejahatan AI di media sosial, khususnya dalam

[1] Jeremiah Maximillian Laza and Rizky Karo Karo, 'PERLINDUNGAN HUKUM TERHADAP ARTIFICIAL INTELLEGENCE DALAM ASPEK PENYALAHGUNAAN DEEPFAKE TECHNOLOGY PADA PERSPEKTIF UU PDP DAN GDPR', *LEX PROSPICIT*, 1.2 (2023).

[2] Wilma Silalahi, Meily Natassya, and Shane Evelina, 'Penggunaan Deepfake Terkait Penyebaran Isu Hoaks Pada Masa Kampanye Pemilu 2024', *Jurnal Bawaslu Provinsi Kepulauan Riau*, 6.1 (2024), 30–45.

konteks penyebaran hoaks dan manipulasi opini publik di masa demonstrasi. Kasian ini bertujuan untuk mengidentifikasi bentuk dan modus operasi kejahatan berbasis AI khusunya *deep fake*, serta menganalisis bagaimana hukum positif di Indonesia mengatur dan menanggapi fenomena tersebut. Selain itu, penelitian ini juga ingin mengkaji tanggung jawab hukum pelaku, pengembang, dan platform media sosial dalam menghadapi penyalahgunaan AI. Penelitian ini diharapkan dapat memberikan kontribusi nyata dalam pengembangan hukum siber di Indonesia dan menjadi acuan bagi perumusan kebijakan yang lebih adaptif terhadap kemajuan teknologi.

METODE

Kajian ini menggunakan metode penelitian hukum yuridis normatif yang mana objek yang menjadi kajian dalam hal ini berkaitan dengan peraturan perundang-undangan. Sebagaimana objek dalam kajian ini berkaitan dengan peraturan perundang-undangan maka selanjutnya pendekatan yang digunakan adalah pendekatan perundang-undangan. Peraturan perundang-undangan yang akan digunakan dalam kajian ini adalah Undang-Undang Nomor 1 Tahun 1946 Tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang kemudian diubah dengan Udnang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana, dan Peraturan Mahkamah Agung Nomor 4 tahun 2016 Tentang Tata Cara Pemeriksaan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik. Selanjutnya dalam penegumpulan bahan hukum akan dilakukan dengan studi kepustakaan yakni melakukan penelusuran atau membaca di internet maupun perpustakaan yang kemudian akan dilakukan analisis lebih lanjut.

HASIL DAN PEMBAHASAN

A. Bentuk- bentuk Deepfake sebagai kejahatan berbasis AI untuk Penyebaran Berita Bohong di Media Sosial

Perkembangan teknologi pada saat ini menunjukkan kemajuan yang sangat besar terutama dengan munculnya Kecerdasan Buatan atau AI yang kemudian pengunaan AI ini meningkat sangat cepat yang ditandai dengan Indonesia merupakan negara dengan penggunaan AI tertinggi sebesar 24,6%

berdasarkan survey IDC Asia Pacific 2018 [3]. Berdasarkan data yang menunjukkan tingginya penggunaan AI di Indonesia ini tidak hanya mengarah pada dampak positif tentu dariapda itu tidak dapat disangkal terkait dampak negatif yang ditimbulkan, dampak negatif tersebut tidak secara langsung ditimbulkan oleh AI namun oleh penggunanya yang menyalahgunakan AI untuk melakukan kejahatan. Pengguna internet Indonesia pada tahun 2023 menunjukkan sebanyak 73,7% dari total populasi di Indonesia pada tahun tersebut [4]. Banyaknya jumlah pengguna internet menunjukkan bahwa internet ini kemudian menjadi bagian besar yang tidak dapat terlepas dari kehidupan masyarakat. Seiring dengan berkembangnya teknologi tersebut, terdapat perubahan yang terjadi di masyarakat dalam kehidupan sehari-hari seperti halnya berkaitan dengan penyebaran informasi dulunya masih menggunakan koran atau majalah yang kemudian dengan memanfaatkan teknologi saat ini penyebaran informasi di era digital beralih melalui media sosial.

Artificial Intelligence (AI) atau yang biasa disebut dengan Kecerdasan Buatan adalah suatu bentuk dari kemajuan teknologi yang fungsinya diciptakan untuk meniru fungsi kognitif manusia yang basis sistemnya seperti menganalisis data, memahami pola, mengenali lingkungan sekitar hingga membuat suatu keputusan [5]. Sistem dalam AI ini akan mengolah informasi yang dimasukan dengan algoritma yang telah diprogramkan untuk memberikan atau menentukan suatu hasil [6]. Kejahatan berbasis AI ini dapat berupa banyak bentuk dan dengan modus yang beragam dikarenakan AI sendiri seperti yang telah dijelaskan merupakan suatu produk dari kemajuan teknologi dan memiliki sistem untuk menganalisis data dan sebagainya sehingga lebih canggih. Kecerdasan buatan atau AI ini dapat dikatakan sebagai pisau bermata dua dikarenakan disamping adanya manfaat atau kelebihan yang diberikan oleh AI dalam membantu kehidupan manusia

[3] Adnasohn Aqilla Respati, 'Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation', *Jurnal USM Law Review*, 7.3 (2024), 4–12.

[4] Bilqist Izdihar, 'Cyberlaw as a Tool to Control the Spread of Hoaxes on Social Media', *Jurnal Hukum Mimbar Justitia (JHMJ)*, 10.2 (2024), 211–22.

[5] Budi Pramono and Lukman Yudho Prakoso, 'Antisipasi Pertahanan Dan Keamanan Cyberpolitics Dengan Artificial Intelligence', *Jurnal Review Politik*, 12.2 (2022), 196–210.

[6] Kurnia Dewi Anggraeny, Mufti Khakim, and Muhammad Rizal Sirojudin, 'The Urgency of Cybercrime Law Reform in Indonesia : Resolving Artificial Intelligence Criminal Liability', *JUSTISI*, 11.1 (2025), 111–26.

kesehariannya namun juga terdapat risiko adanya penyalahgunaan AI untuk melakukan kejahatan sehingga dalam hal ini terdapat dua sisi yang perlu dipertimbangkan dalam penggunaan AI. AI sering kali digunakan untuk melakukan kejahatan siber yang disebut dengan *deepfake* (konten palsu). Deepfake ini merupakan suatu contoh dari perkembangan teknologi yang semakin pesat yang di dalamnya kemudian memanfaatkan algoritma *machine learning* untuk menggabungkan elemen dari berbagai gambar atau video sehingga dapat menciptakan suatu konten yang tampak nyata [7]. *The term "deep fake" originates from a combination of the words "deep learning" and "fake"* yang apabila diartikan berarti bahwa istilah *"deep fake"* ini berasal dari gabungan kata *"deep learning"* dan *"fake"* [8]. Istilah *deepfake* sendiri sebenarnya sudah menunjukkan apa yang dimaksud dengan *deepfake* yang mana *deepfake* ini terdiri dari kata *fake* yang berarti palsu maka jelas bahwa *deepfake* ini merupakan suatu bentuk dari perkembangan teknologi yang digunakan untuk menciptakan suatu hal yang palsu atau tidak asli yang dalam hal ini karena ia merupakan gabungan juga dari kata *deep learning* maka dalam proses pembuatan suatu konten palsu tersebut akan melibatkan *deep learning* untuk dapat menghasilkan suatu konten palsu yang terlihat nyata.

Berdasarkan data Kementrian Komunikasi dan Informatika mencatat lebih dari 1.800 kasus penyebaran hoaks pada berbagai macam platform media sosial sepanjang tahun 2022 dengan dampak signifikan yang ditimbulkan dari penyebaran hoaks tersebut mengarah pada polarisasi masyarakat dan stabilitas sosial-politik [9]. Data kasus penyebaran hoaks tersebut dapat dikatakan sebagai bukti kejahatan siber yang kian marak terjadi sebagai dampak negatif yang ditimbulkan oleh pengguna internet yang menyalahgunakan internet untuk dijadikan alat melakukan kejahatan. Penyebaran hoaks atau berita bohong melalui media sosial ini berbeda dengan melalui koran dikarenakan dengan kemudahan yang diberikan oleh

[7] Riski Septiawan, 'CRITICAL ANALYSIS OF AI-PRODUCED MEDIA: A STUDY OF THE IMPLICATIONS OF DEEPFAKE TECHNOLOGY', *DEVOTION Journal of Research and Community Service*, 5.7 (2024), 735–41.

[8] Ari Purwadi and Cita Yustisia Serfiyani, 'Legal Landscape on National Cybersecurity Capacity in Combating Cyberterrorism Using Deep Fake Technology in Indonesia', *International Journal of Cyber Criminology*, 16.1 (2022), 123–40 <https://doi.org/10.5281/zenodo.4766560>.

[9] Izdihar, Bilqist, 'Cyberlaw as a Tool to Control the Spread of Hoaxes on Social Media', *Jurnal Hukum Mimbar Justitia (JHMJ)*, 10.2 (2024), Hal 211–22

teknologi dalam era digital kemudian tidak terbatas wilayah atau geografis ini membuat penyebaran hoaks lebih cepat dan masif langsung ke banyak orang sekaligus. Kecepatan penyebaran informasi melalui media sosial tersebut memungkian juga untuk penyebaran hoaks meningkat yang mana bahkan dalam kurun waktu yang tidak lama suatu konten yang berisikan hoaks dapat diakses atau dibaca oleh ratusan hingga ribuan pengguna media sosial. Selanjutnya berkaitan dengan penyebaran hoaks yang secara cepat melalui media sosial ini tidak lain dikarenakan banyak sekali jumlah pengguna media sosial sehingga suatu informasi yang beredar di media sosial akan dapat diakses oleh semua pengguna media sosial kemudian para pengguna media sosial juga dapat meneruskan penyebaran berita hoaks tersebut ke pengguna lainnya sebagaimana terdapat beberapa proses penyebaran hoaks dapat terjadi. Penyebaran hoaks pada dasarnya dapat terjadi secara cepat melalui media sosial dikarenakan tidak hanya disebarkan oleh pelaku yang memang sengaja membuat berita bohong kemudian menyebarkannya ke media sosial atau yang kedua adalah ketika pengguna media sosial secara tidak sengaja telah menyebarkan berita hoaks dikarenakan ia sendiri tidak mengetahui bahwa berita tersebut merupakan berita hoaks sehingga pengguna tersebut mengira hanya membagikan informasi yang dikiranya benar. Apabila merujuk pada data dari BPS pada tahun 2021 ada sebanyak 88,89% pengguna internet di Indonesia yang mengakses media sosial yang berasal mulai dari kelompok usia 5 (lima) tahun ke atas [10]. Meninjau dari data tersebut maka dapat dikatakan bahwa media sosial ini sangat berpengaruh pada kehidupan manusia bahkan sejak dari usia dini sehingga memang jangkauan media sosial ini luar biasa tidak terbatas usia yang mana hal tersebut juga menyebabkan berita atau informasi palsu dapat diterima oleh anak-anak yang nantinya dapat berpengaruh pada perubahan pola pikir dan perilaku anak. Sebagaimana sudah dijelaskan sebelumnya bahwa *deepfake* ini dapat meniru atau menyamai baik dari segi audio atau visual yang dalam hal ini seperti halnya wajah atau suara seseorang maka dalam penggunaan *deepfake* ini tentu diperlukan beberapa tahapan untuk proses menghasilkan suatu konten yang realistik atau hampir sangat nyata. Tahapan dalam membuat suatu konten *face swap deepfake* dimulai dengan pengumpulan data wajah yang akan digunakan baik dalam

[10] Anissa Larasati, 'Perlindungan Hukum Anak Dalam Penggunaan Media Sosial: Mendesak Penguatan Regulasi Pembatasan Usia Di Indonesia', *MARINews*, 2025 <https://marinews.mahkamahagung.go.id/artikel/perlindungan-hukum-anak-dalam-penggunaan-media-sosial-07j>.

bentuk gambar atau video yang wajah seseorang dapat terlihat dengan jelas, selanjutnya akan dilakukan pengenalan wajah dengan menggunakan algoritma *machine learning* untuk mengidentifikasi fitur wajah unik yang memungkinkan untuk penggantian wajah. Tahapan yang ketiga adalah mengganti wajah atau memasangkan wajah pada wajah orang lain dengan menggunakan algortima *machine learning* yang selanjutnya akan diikuti dengan sinkronisasi gerakan bibir dan mata untuk menciptakan efek yang menyerupai orang berbicara. Tahap terakhir yaitu video atau gambar yang sudah dihasilkan sebelumnya diedit untuk menciptakan efek yang menyerupai aslinya. Teknologi yang digunakan dalam pembuatan *face swap deepfake* ini melibatkan machine learning seperti *Generative Adversarial Networks (GAN)* dan *Convolutional Neural CNN* yang mana keduanya ini berfungsi dalam hal untuk mengenali fitur wajah yang unik [11]. Jadi dengan adanya *face swap deepfake* ini, individu yang sebelumnya tidak pernah melakukan suatu hal kemudian wajah dari individu tersebut diambil atau dipasang menggantikan wajah orang lain yang seolah-olah benar bahwa individu tersebut memang melakukan hal yang dimaksud.

Salah satu bentuk deepfake lainnya yakni *voice cloning* atau dapat juga dikatakan sebagai *deepfake audio* yaitu berupa peniruan suara seseorang yang dalam prosesnya melibatkan deep learning agar dapat memanipulasi suara untuk membuat suara yang sama terdengar seperti aslinya tetapi dengan informasi yang berbeda dengan yang sebenarnya. Pembuatan deepfake audio ini sebagaimana yang disebutkan sebelumnya yakni dengan menggunakan deep learning seperti *Neural Networks* terkait dengan model dari intonasi, vokal, dan nuansa suara sehingga dapa terdengar seperti suara aslinya. Hampir sama seperti *face swap deepfake*, untuk *audio deepfake* ini juga memerlukan beberapa tahapan dalam pembuatannya yang dimulai dari pengumpulan suara dari individu yang ingin dimanipulasi atau subjek yang menjadi target, kemudian dilanjutkan dengan pemodelan menggunakan *deep learning* untuk menciptakan suara seperti individu yang ingin dimanipulasi [12]. Peniruan suara atau *voice cloning* ini dapat digunakan dalam penyebaran hoaks yang mana suara yang ditiru adalah suara dari seseorang penting yang memiliki pengaruh di masyarakat atau tokoh tokoh lainnya kemudian dengan

[11] Septiawan, Riski, 'CRITICAL ANALYSIS OF AI-PRODUCED MEDIA: A STUDY OF THE IMPLICATIONS OF DEEPFAKE TECHNOLOGY', *DEVOTION Journal of Research and Community Service*, 5.7 (2024), Hal. 735–41

[12] Ibid.

suara tiruan tersebut disampaikan suatu informasi bohong untuk memanipulasi opini publik, dengan pernyataan yang dianggap asli disampaikan oleh tokoh penting tersebut kemudian terdapat masyarakat yang mungkin bisa saja setuju maupun tidak sehingga terjadi konflik opini antar masyarakat. Selanjutnya *voice cloning* yang termasuk dalam salah satu bentuk dari *deepfake* ini sangat berbahaya oleh karena itu perlu untuk diperhatikan lebih lanjut dikarenakan dapat memberikan informasi yang salah atau hoaks dengan menirukan suara seorang tokoh yang berpengaruh dengan tujuan untuk menipu orang lain.

Deepfake ini juga meliputi *deepfake lip-sync* yang mana *deepfake* ini akan membuat Gerakan bibir dalam suatu video sesuai dengan audio yang dihasilkan secara tepat. Proses dalam pembuatan *deepfake lip-sync* ini menggunakan *deep learning* seperti *Long Short-Term Memory (LSTM)* atau *transformer-based models* untuk menciptakan sinkronisasi yang akurat. Pembuatan *deepfake lip-sync* ini menggunakan *deep learning* untuk dapat mendeteksi, memahami, dan mereplikasi gerakan bibir dan wajah dari satu video ke video yang lain [13]. Suatu konten yang tujuannya dibuat untuk seperti nyata maka diperlukan juga untuk terdapat sinkronisasi yang tepat antara audio atau suara dengan gerakan bibir sehingga kemudian kesesuaian antara gerakan bibir dan audio dalam suatu video sangatlah penting dikarenakan apabila di natara keduanya tidak ada kesesuaian maka dapat diketahui bahwa konten tersebut palsu atau bohong oleh karena itu seseorang yang menggunakan *deepfake* untuk tujuan tidak baik akan berusaha untuk dapat menghasilkan suatu konten yang dapat dipercayai oleh orang lain agar tujuan jahatnya terpenuhi. Adanya *deepfake lip-sync* ini kemudian melengkapi *face swap deepfake* dan *audio deepfake* sehingga memunculkan suatu konten yang terlihat seperti suatu video yang jelas dan nyata benar benar ada dengan audio dan gerakan bibir yang sesuai sehingga sulit bagi banyak orang untuk mengenali bahwa konten tersebut bohong atau palsu.

Perkembangan teknologi memiliki pengaruh yang signifikan terhadap struktur sosial, ekonomi, dan hukum sebagaimana yang dimaksud dalam teori *Technological Determinism* [14]. Penyalahgunaan AI untuk melakukan *deepfake* dapat berpengaruh pada ketertiban umum atau keamanan negara yakni dengan penyebaran konten palsu atau disinformasi

[13] Ibid.

[14] Wahyudi Br, 'Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI', *INNOVATIVE: Journal Of Social Science Research*, 5.1 (2025).

politik atau isu sosial yang dihasilkan oleh *deepfake* dapat menyebabkan adanya manipulasi opini masyarakat terhadap satu pihak sehingga terjadi kesalahpahaman yang berkibat buruk pada tatanan sosial dan politik suatu negara sebagaimana hal ini sesuai dengan teori Tecnological Determinism yang disebutkan sebelumnya sehingga pengaruh dari kejahatan berbasis AI ini tidak hanya pada satu individu saja namun juga secara menyeluruh dapat menyebabkan rusaknya suatu struktur atau tatanan sosial maupun hukum. Kejahatan berbasis AI *Deepfake* ini dapat dikatakan memanfaatkan teknologi audio visual yang kemudian memungkinkan agar seseorang dapat memanipulasi baik itu gambar atau suara yang dapat meniru bentuk wajah atau suara individu tertentu secara meyakinkan untuk dijadikan konten yang tidak benar atau bohong dan disebarluaskan di media sosial yang sebenarnya individu yang ditiru tidak pernah melakukan atau membuat konten tersebut. Kemajuan teknologi yang berdampak pada perkembangan penyebaran informasi palsu ditunjukkan dengan yang dulunya penyebaran berita hoaks hanya berbentuk teks atau gambar saja namun saat ini penyebaran hoaks dapat melalui video yang mana video tersebut dibuat dengan *deepfake* yang hasilnya sangat meyakinkan dan sulit untuk dikenali atau diketahui bahwa video tersebut palsu kemudian juga karena media sosial ini tidak dibatasi oleh wilayah sehingga penyebaran hoaks kemudian menjadi sangat mudah untuk diterima dan dipercayai oleh masyarakat. Sebagaimana disebutkan bahwa salah satu alasan mengapa penyeberan hoaks menggunakan *deepfake* di media sosial ini dapat tersebar sangat cepat dan diketahui banyak orang dalam waktu singkat dikarenakan media sosial ini tidak terbatasi oleh wilayah sehingga media sosial ini dapat menjangkau banyak orang di dunia bahkan hingga wilayah-wilayah kecil, berdasarkan hal tersebut maka dapat dikatakan bahwa penggunaan *deepfake* untuk menyebarkan hoaks sesuai dengan Teori *Cross Boarder Crime*. Teori *Cross Boarder Crime* sendiri berkaitan dengan kejahatan lintas batas yang mencakup sejumlah atau segala aktivitas kejahatan yang dilakukan baik oleh individu ataupun kelompok yang tersebar baik secara nasional atau internasional dengan keuntungan yang diharapkan adalah terkait finansial atau sosial-politik, dan lainnya [15]. Apabila merujuk dari teori tersebut maka sesuai dengan karakteristik dari penyebaran hoak menggunakan *deepfake* di media sosial yang pelakunya dapat seorang individua tau kelompok kemudian konten *deepfake* tersebut

[15] Mim Sertaç Tümtaş and Yosra JARRAR, *International Symposium on Strategic and Social Research Full Text Book*, 2022.

tidak hanya tersebar nasional saja namun juga internasional yang mana dalam hal ini konten *deepfake* tersebut juga dapat digunakan berkaitan dengan sosial-politik dengan tujuan untuk memanipulasi opini publik terhadap politik suatu negara.

The following deep fake character is that the primary purpose of making videos is to influence people's mindsets through the concept of "seeing is believing" apabila diartikan berarti bahwa karakteristik dari deep fake adalah tujuan utama dari pembuatan video menggunakan deepfake tersebut yakni untuk memengaruhi pola pikir orang melalui konsep "melihat adalah percaya" [16]. Sebagaimana disebutkan bahwa tujuan utama daripada *deep fake* sendiri adalah untuk mengubah pola pikir seseorang melalui konsep melihat adalah percaya maka dapat dikatakan bahwa semua konten yang dihasilkan dengan menggunakan *deepfake* ini ingin memastikan bahwa seseorang dapat mempercayai konten yang dilihatnya dimana deepfake ini menghasilkan suatu koten yang mulai dari bentuk wajah, suara, maupun bentuk bibir ini sesuai dan menyerupai orang aslinya yang selanjutnya konten tersebut berisikan suatu informasi tidak benar tujuannya agar dapat mengubah pola pikir orang banyak dengan maksud tertentu. Sering kalinya *deepfake* ini juga ditujukan untuk membuat disinformasi politik dengan menyebarkan informasi yang tidak benar yang dirancang untuk sengaja merusak kredibilitas dari tokoh politik tertentu atau tidak hanya politik namun juga terkait keamanan negara yakni dengan ditujukan pada aparat penegak hukum agar terjadi konflik antara penegak hukum dan masyarakat lebih lanjut sebagaimana yang kita tahu bahwa keamanan nasional tidak hanya kaitannya dengan militer akan tetapi juga mencakup beberapa aspek lainnya baik aspek sosial, politik maupun tanggapan atau reaksi masyarakat publik terhadap negara. Indonesia sebagai negara demokrasi memiliki tantangan literasi media dengan adanya *deepfake* yang memiliki potensi menciptakan ketidakpastian massal pada ruang publik yang dapat mengakibatkan rentannya instabilitas sosial dan politik dikarenakan *deepfake* memberikan pengaruh pada sikap warga terhadap otoritas ataupun berita dari disorientasi informasi [17]. Fenomena *deepfake* ini menimbulkan keresahan

[16] Purwadi, Ari, and Cita Yustisia Serfiyani. 2022. "Legal Landscape on National Cybersecurity Capacity in Combating Cyberterrorism Using Deep Fake Technology in Indonesia." *International Journal of Cyber Criminology* 16(1):123–40. doi: 10.5281/zenodo.4766560

[17] Sri Wahyuni Nurdin and Imam Fadhil Nugraha, 'ANCAMAN DEEPFAKE DAN DISINFORMASI BERBASIS AI: IMPLIKASI TERHADAP KEAMANAN SIBER DAN STABILITAS NASIONAL INDONESIA', *JIMR: Journal Of International Multidisciplinary Research*, 4.01 (2025), 73–92.

dalam masyarakat dengan membuat narasi palsu, menyebarkan propaganda dan dapat mengganggu atau membuat rentan proses demokratisasi karena dapat menciptakan konflik dan menyebabkan penurunan kepercayaan publik terhadap institusi-institusi formal seperti penegak hukum atau bahkan Pemerintah apabila berkaitan dengan berita bohong dikarenakan *deepfake* tersebut dapat meniru secara meyakinkan yang akhirnya masyarakat pengguna internet atau media sosial kesulitan untuk membedakan apakah konten tersebut asli atau palsu disebabkan oleh batas antara yang secara faktual benar dan fiktif ini menjadi kabur sehingga di sini penting adanya literasi digital lebih lanjut agar dengan adanya konten palsu yang tersebar luas di media sosial dapat disaring oleh masyarakat itu sendiri dengan memverifikasi apakah konten tersebut benar asli atau tidak. Menurut catatan INDEF menunjukkan tingkat literasi digital di Indonesia hanya sebesar 62% [18]. Menjadi permasalahan selanjutnya yang ditunjukkan dengan data tersebut adalah ketika masyarakat sendiri masih kesulitan untuk dapat membedakan antara konten asli dan konten yang memuat berita bohong dikarenakan kurangnya literasi digital sehingga inilah yang kemudian menyebabkan penyebaran hoaks yang tidak disengaja terus menerus terjadi.

Penyebaran Hoaks melalui *deepfake* menjadi sangat berbahaya dan masih terus menerus ada serta memiliki peran besar dalam pengaruh sikap atau opini publik apabila masyarakat masih memiliki keterbatasan kemampuan untuk memverifikasi informasi secara mandiri sehingga secara berkelanjutan masih terdapat beberapa masyarakat yang menerima informasi secara langsung tanpa memahami terlebih dahulu kebenarannya. Selanjutnya yang menjadikan keberadaan *deepfake* ini semakin berdampak adalah bahwa publik saat ini memiliki keraguan terhadap konten-konten yang beredar di media sosial, dalam hal ini tidak hanya konten palsu yang dipertanyakan tetapi termasuk yang resmi atau benar, dengan adanya keraguan pada konten resmi maka akan menimbulkan konflik yang tidak terselesaikan. Pengaruh *deepfake* terhadap kerentanan proses demokratisasi dapat dilihat dengan adanya video hoaks yang seringkali tersebar pada saat aksi demonstrasi sehingga menciptakan propaganda untuk menciptakan konflik antara demonstran dan aparat penegak hukum. Pemahaman selanjutnya terkait kejahatan siber berbasis AI seperti *deepfake* ini dapat memicu adanya

[18] Adyaksa Vidi, 'Hoaks Pakai Teknologi Deepfake Makin Marak, Masyarakat Dituntut Jeli Cerna Informasi', *Liputan 6*, 2025 <https://www.liputan6.com/cek-fakta/read/6178364/hoaks-pakai-teknologi-deepfake-makin-marak-masyarakat-dituntut-jeli-cerna-informasi>.

demonstrasi, dimana salah satu strateginya adalah dalam pemanfaatan media sosial untuk penyebaran konten *deepfake* yang berisikan informasi bohong berkaitan dengan isu sosial politik untuk memengaruhi banyak orang yang melihat konten tersebut kemudian mempercayai konten tersebut tanpa memastikan terlebih dahulu keaslian dari konten tersebut. Oleh karena itu banyak orang yang melihat konten *deepfake* namun menganggap bahwa konten tersebut asli atau benar sehingga di sini *deepfake* berhasil membuat suatu propaganda dalam keadaan tertentu. Saat ini dapat dikatakan bahwa media sosial merupakan suatu sarana penyebarluasan informasi yang efektif sehingga *deepfake* ini kemudian banyak disebarluaskan di media sosial dengan pandangan bahwa media sosial merupakan bagian penting yang memiliki peran untuk dapat dimanfaatkan guna mendominasi atau memanipulasi opini publik di dunia maya sebagaimana data sebelumnya menunjukkan banyaknya jumlah masyarakat yang menggunakan media sosial ini mempermudah penyebaran hoaks dengan *deepfake* untuk dapat menjangkau orang banyak dalam waktu yang singkat. *Deepfake* yang menyangkut isu sosial politik ini digunakan untuk menciptakan suatu propaganda dalam suatu negara yang tujuannya adalah tidak lain untuk dapat memecah belah persatuan masyarakat. Media sosial ini yang merupakan alat untuk komunikasi massa selanjutnya digunakan oleh individu atau kelompok sebagai salah satu media dalam menyebarkan suatu keyakinan atau doktrin yang tidak sesuai. Dalam konten *deepfake* biasanya yang dijadikan sebagai sorotan adalah berkaitan dengan kerusuhan atau isu isu politik yang sedang panas dan banyak dibahas dalam masyarakat, salah satunya seperti pemilihan umum, aksi demonstrasi atau isu antara kesewenangan pemerintah terhadap masyarakat yang mana informasi dalam konten tersebut dapat didasarkan pada informasi asli yang dikurangi atau dilebih-lebihkan atau bahkan seluruhnya merupakan informasi tidak benar. Berdasarkan penjelasan tersebut maka selanjutnya dapat disimpulkan bahwa penggunaan deepfake dalam penyebaran berita hoaks dapat menganggu atau menghalangi Pertahanan Negara sebagaimana Pertahanan Negara diartikan dalam Pasal 1 angka 1 Undang-Undang Nomor 3 tahun 2002 Tentang Pertahanan Negara sebagai segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara [19].

[19] Republik Indonesia, *UNDANG-UNDANG RI NOMOR 3 TAHUN 2002 TENTANG PERTAHANAN NEGARA* (Indonesia, 2002).

Apabila pengertian daripada pertahanan negara adalah pada intinya uapaya untuk melindungi negara kedaulatan dan keutuhan negara maka dengan adanya penggunaan *deepfake* untuk penyebaran berita hoaks tentu akan berpengaruh terhadap pertahanan negara yang mana berita hoaks tersebut seringkalinya menyebabkan propaganda yang akhirnya berakhir pada kerusuhan antar warga negara atau wara negara dengan aparat penegak hukum sehingga keutuhan bangsa dan negara ini sendiri dapat terancam. Kerusuhan antar warga negara ini dapat terjadi dalam hal Pemilihan Umum yang mana satu warga negara dan yang lain memiliki perbedaan untuk Paslon yang didukung, kemudian terdapat berita hoaks terhadap salah satu Paslon mengakibatkan antar warga yang berbeda pilihan tersebut kemudian saling bertentangan opini terhadap berita hoaks tersebut hingga akhirnya dapat berujung pada kerusuhan. Sedangkan kerusuhan antara warga dengan aparat penegak hukum dapat terjadi dalam hal terdapat berita hoaks penyalahgunaan wewenang oleh aparat penegak hukum terhadap salah satu warga sehingga warga tersebut dirugikan akan memancing warga negara untuk mengutarakan rasa kebencian terhadap aparat tersebut dan dapat melakukan unjuk rasa yang tidak sesuai dengan fakta yang sebenarnya, selain itu ketika aksi demonstrasi terjadi ini tidak sedikit berita hoaks yang tersebar yang menjelekkan aparat atau warga selanjutnya akan memprovokasi adanya bentrok antar keduanya.

Modusnya penggunaan konten *deepfake* ini dilakukan dengan penyebaran konten secara masif atau membuat tagar yang menarik agar menjadi viral atau topik *trending* sebagaimana yang kita tahu bahwa apabila konten tersebut menjadi trending maka jumlah penonton yang melihat konten tersebut sangatlah banyak dan bagi yang kurang literasi digital akan dapat terpengaruh secara langsung oleh konten *deepfake* tersebut. Informasi yang disampaikan atau disebarkan dalam konten *deepfake* ini juga dapat dibilang biasanya memberikan keuntungan pada suatu pihak tertentu yang mana keuntungan tersebut didapatkan dengan menjelekkan individu lain melalui informasi tidak benar agar masyarakat yang sebelumnya mendukung individu tersebut beralih ke pihak yang diuntungkan. Praktik semacam ini, akan menimbulkan mispresepsi dalam masyarakat yang pada akhirnya akan berakibat pada terjadinya aksi demonstrasi yang dipicu dari informasi bohong dari *deepfake* yang membuat masyarakat percaya bahwa informasi tersebut sehingga menimbulkan kemarahan dan kerusuhan pada suatu negara. Berdasarkan Laporan Risiko Global 2025 oleh World Economic Forum menempatkan misinformasi dan disinformasi sebagai ancaman global nomor 4 dan diprediksi dapat menjadi ancaman global nomor satu pada tahun

2027 yang mana laporan tersebut didasarkan pada survei terhadap lebih dari 900 pakar internasional lintas sektor [20]. Melihat dari data tersebut maka dapat diketahui bahwa penyebaran hoaks yang dapat menyebabkan misinformasi dan disinformasi merupakan suatu ancaman global yang nantinya akan berpengaruh besar dalam stabilitas kehidupan antar negara, hal tersebut menunjukkan bahwa adanya misinformasi dan disinformasi yang kian terus menerus masih banyak beredar di media sosial atau internet memiliki dampak yang buruk terhadap manusia itu sendiri. Upaya untuk menghilangkan atau mengurangi penyebaran berita hoaks kemudian menjadi sangat penting guna kepentingan bersama.

B. Dampak kejahatan AI (deep fake) dalam keamanan negara

Kejahatan berbasis kecerdasan buatan (Artificial Intelligence/AI), khususnya teknologi *deepfake*, telah berkembang menjadi ancaman nyata terhadap keamanan negara di era digital. *Deepfake* memungkinkan manipulasi visual dan audio dengan tingkat realisme yang sangat tinggi, sehingga sulit dibedakan dari konten asli. Teknologi ini dapat digunakan untuk menciptakan pernyataan palsu yang seolah-olah berasal dari pejabat tinggi negara, aparat militer, atau pemimpin politik. Akibatnya, masyarakat dapat dengan mudah terprovokasi oleh informasi yang tidak benar. Dalam jangka panjang, kondisi ini berpotensi merusak legitimasi pemerintah dan menurunkan kepercayaan publik terhadap institusi negara. Jika dibiarkan tanpa pengawasan yang memadai, *deepfake* dapat menjadi alat destabilisasi yang serius bagi keamanan nasional.

Penyebaran berita hoaks yang memanfaatkan *deepfake* menjadi salah satu bentuk ancaman paling berbahaya dalam ruang siber. Konten hoaks berbasis AI sering kali dirancang secara sistematis untuk mempengaruhi emosi publik, seperti ketakutan, kemarahan, atau kebencian. Hoaks semacam ini dapat menyebar dengan cepat melalui media sosial, aplikasi pesan instan, dan platform digital lainnya. Dalam konteks keamanan negara, penyebaran hoaks dapat memicu konflik sosial, perpecahan politik, serta ketidakstabilan keamanan dalam negeri. Situasi ini dapat dimanfaatkan oleh aktor internal maupun eksternal untuk melemahkan persatuan nasional. Oleh karena itu, hoaks berbasis deep fake menjadi ancaman strategis yang harus ditangani secara serius oleh negara.

[20] Vidi, Adyaksa, 'Hoaks Pakai Teknologi Deepfake Makin Marak, Masyarakat Dituntut Jeli Cerna Informasi', *Liputan 6*, 2025 <https://www.liputan6.com/cek-fakta/read/6178364/hoaks-pakai-teknologi-deepfake-makin-marak-masyarakat-dituntut-jeli-cerna-informasi>

Pemahaman selanjutnya terkait kejahatan siber *text generative AI* berupa bot yang dapat memicu demonstrasi, serangan bot ini biasanya dilakukan pada akun akun media sosial, dimana salah satu strategi dalam pemanfaatan media sosial ialah sebagai penyebarluasan informasi. Bot merupakan suatu program komputer yang dijalankan dengan otomatis yang memanfaatkan teknologi AI, dimana karakter bot ini memiliki pola aktivitas yang seragam dan cenderung kaku dengan tujuan untuk membuat suatu propaganda atau memantik sentimen masyarakat dalam keadaan tertentu. Saat ini media sosial dianggap sebagai sarana penyebarluasan yang efektif. Bot dipandang sebagai bagian dari salah satu hal yang penting yang dapat dimanfaatkan untuk mendominasi opini di dunia maya, dengan memanfaatkan bot biasanya bisnis bisnis yang menggunakan media sosial untuk mempromosikan produknya dengan memberi *like* atau mengomentari postingan tersebut. Namun dalam ranah politik bot digunakan untuk menciptakan suatu propaganda di berbagai negara yang dapat memecah belah persatuan masyarakat. Propaganda ini terkait suatu bentuk komunikasi massa yang digunakan individua tau kelompok sebagai salah satu media dalam menyebarkan suatu keyakinan atau doktrin. Dalam kasus bot yang dimodifikasi oleh pelaku biasanya menyoroti kerusuhan atau isu isu politik yang sedang panas di masyarakat, salah satunya seperti pemilihan umum, atau isu antara kesewenangan pemerintah terhadap masyarakat.

Modusnya penggunaan bot ini dilakukan dengan penyebaran konten yang masif atau membuat ciri khas dengan tagar agar menjadi viral atau topik *trending.* Informasi yang disebarkan biasanya menguntungkan salah satu pihak dan menjatuhkan pihak lawan. Ciri ciri akun bot biasanya memiliki pengikut yang sedikit dan biasanya akun tersebut baru dibuat. Dalam suatu kasus pada pilpres 2024 setiap pasangan memiliki buzzer dimana praktik buzzer ini digunakan untuk membangun sarana utama yakni narasi politik dan memengaruhi opini publik. Buzzer politik pilpres 2024 sebagian besar terdiri dari akun akun media sosial yang baik dioperasikan secara manual oleh individua tau secara otomatis yakni menggunakan bot, dan mayoritas akun akun yang terlibat dalam aktivitas buzzer adalah akun bot, sementara sisanya dilakukan oleh timses paslon, dan individu lain seperti pendukung asli dari paslon tersebut. bot dalam kampanye buzzer inilah yang menyebarkan konten masif dan cepat sehingga memengaruhi *trending topic* di beberapa media sosial seperti *Twitter, Facebook, Tiktok* dan *Instagram.* Berita berita yang disebarkan juga belum tentu benar dan fakta, sehingga buzzer biasanya tidak segan segan menggunakan taktik politik yang tidak

baik, dengan menyebaarkan hoax, fitnah ataupun serangan pribadi. Praktik semacam ini, yang menimbulkan adanya *miss* persepsi pada masyarakat dan pada akhirnya menimbulkan aksi demonstrasi yang menyebabkan kerusuhan (*cheos*). Praktik semacam ini dapat mencederai tentang integritas demokrasi di Indonesia, yang mana kampanye seharusnya berfokus pada visi misi kandidat namun dibajak oleh oknum oknum yang memnafaatkan teknologi AI dengan bot yang tidak bertanggung jawab. Dalam wawancara dengan beberapa ahli, berupa praktik semacam buzzer dengan bot ini tidak hanya merusak reputasi lawan politik namun juga menurunkan standar moral dalam politik indoensia, yang mana praktik ini seringkali memberikan komentar komentar atau narasi yang memecah belah dan memprovokasi masyarakat.

Selain hoaks, *deepfake* juga berkaitan erat dengan peningkatan **cybercrime** yang menargetkan sistem dan sumber daya negara. Teknologi *deepfake* sering digunakan dalam praktik penipuan digital, pemerasan siber, serta pencurian data penting. Dengan memalsukan identitas pejabat atau aparat keamanan, pelaku dapat melakukan rekayasa sosial untuk mendapatkan akses ke sistem strategis negara. Kejahatan semacam ini dapat mengakibatkan kebocoran data rahasia, gangguan layanan publik, dan kerugian ekonomi yang besar. Dampak tersebut tidak hanya merugikan negara secara finansial, tetapi juga melemahkan pertahanan dan keamanan informasi nasional. Oleh karena itu, cybercrime berbasis AI harus dipandang sebagai ancaman serius terhadap kedaulatan negara. Dalam konteks yang lebih luas, penggunaan *deepfake* dan *cybercrime* dapat berkembang menjadi bentuk *cyberterrorism*. *Cyberterrorism* memanfaatkan teknologi informasi untuk menciptakan rasa takut, kepanikan, dan ketidakstabilan melalui serangan digital. Video deep fake yang menampilkan ancaman teror, konflik bersenjata, atau pernyataan provokatif dapat memicu keresahan masyarakat secara masif. Serangan ini tidak memerlukan kekerasan fisik secara langsung, namun dampaknya dapat melumpuhkan sistem sosial dan politik suatu negara. Dengan demikian, *cyberterrorism* berbasis *deepfake* menjadi ancaman non-konvensional yang sulit dideteksi dan ditanggulangi. Hal ini menuntut negara untuk mengembangkan strategi keamanan siber yang adaptif dan komprehensif.

Keberadaan deep fake dalam praktik *cyberterrorism* menunjukkan perubahan paradigma dalam konsep keamanan negara. Ancaman keamanan tidak lagi hanya berbentuk serangan militer atau fisik, melainkan juga serangan informasi dan psikologis. Manipulasi informasi melalui deep fake dapat merusak stabilitas politik tanpa perlu menggunakan senjata

konvensional. Kepercayaan publik, ketertiban sosial, dan legitimasi pemerintah menjadi target utama dalam serangan ini. Jika negara gagal mengendalikan ruang informasi digital, maka risiko instabilitas nasional akan semakin besar. Oleh karena itu, perlindungan keamanan negara harus mencakup dimensi digital dan informasi secara menyeluruh.

Fenomena kejahatan deep fake dan cyberterrorism dapat dianalisis melalui teori *cross border crime* (kejahatan lintas batas negara). Teori ini menjelaskan bahwa kejahatan modern, khususnya kejahatan siber, tidak lagi terikat oleh batas geografis suatu negara. Pelaku kejahatan *deepfake* dapat beroperasi dari negara lain dengan target negara yang berbeda. Hal ini menyebabkan kompleksitas dalam proses penegakan hukum karena perbedaan yurisdiksi, sistem hukum, dan kepentingan politik antarnegara. Dalam konteks keamanan negara, kejahatan lintas batas ini memperbesar risiko ancaman yang sulit dikendalikan secara nasional. Oleh sebab itu, kejahatan AI harus dipahami sebagai masalah global, bukan hanya domestik.

C. Analisis Yuridis terhadap Tindak Kejahatan AI

Perkembangan kecerdasan buatan (*Artificial Intelligence*/AI) telah menimbulkan dimensi baru dalam ranah kejahatan siber (*cybercrime*), terutama ketika teknologi tersebut dimanfaatkan untuk menyebarkan hoaks dan memanipulasi opini publik di media sosial. Dalam konteks hukum Indonesia, tindak kejahatan seperti ini secara umum dapat dijerat dengan ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Namun, penggunaan AI sebagai alat atau pelaku non-manusia dalam tindak pidana menimbulkan problem yuridis baru, khususnya dalam hal pembuktian, pertanggungjawaban hukum, dan penentuan subjek hukum yang bertanggung jawab. Karakter AI yang bersifat otonom dan adaptif menyebabkan batas antara pelaku manusia dan sistem menjadi kabur.

Secara normatif, Pasal 28 ayat (1) UU ITE mengatur bahwa *"Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dapat dipidana."* Sementara itu, Pasal 28 ayat (2) melarang penyebaran informasi yang menimbulkan kebencian atau permusuhan berdasarkan SARA. Ketentuan ini dapat digunakan untuk menjerat individu atau kelompok yang secara sengaja menggunakan AI untuk menciptakan dan menyebarkan konten palsu seperti *deepfake*, teks manipulatif, atau kampanye opini yang menyesatkan. Namun, jika AI bekerja secara otomatis tanpa

instruksi langsung dari pengguna, maka unsur kesengajaan (*mens rea*) dalam pasal tersebut menjadi sulit dibuktikan, sehingga ruang penegakan hukumnya menjadi terbatas.

Selain UU ITE, pengaturan mengenai kejahatan berbasis AI juga dapat ditinjau dari Kitab Undang-Undang Hukum Pidana (KUHP), khususnya Pasal 55 dan 56 tentang penyertaan (*deelneming*) yang mengatur pertanggungjawaban terhadap pihak yang turut serta melakukan, menyuruh melakukan, atau membantu terjadinya tindak pidana. Dalam konteks AI, pihak yang mengoperasikan atau memprogram sistem untuk tujuan menyebarkan hoaks dapat dianggap sebagai pelaku tidak langsung. Pasal ini menjadi relevan karena AI sendiri belum diakui sebagai subjek hukum, sehingga tanggung jawab tetap dibebankan pada manusia di balik sistem tersebut. Dengan demikian, AI berperan sebagai "alat kejahatan digital" yang digunakan oleh pelaku manusia, bukan sebagai entitas hukum yang berdiri sendiri.

Dari perspektif perlindungan data dan informasi pribadi, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) juga memiliki relevansi. Pasal 65 dan 66 UU PDP menegaskan kewajiban pengendali data untuk menjaga keamanan dan mencegah penyalahgunaan data pribadi. Ketika AI digunakan untuk memanipulasi data, membuat identitas palsu, atau meniru wajah seseorang dalam konten *deepfake*, maka pelaku dapat dijerat dengan ketentuan ini. Pelanggaran terhadap prinsip-prinsip perlindungan data juga dapat menimbulkan tanggung jawab hukum perdata dan administratif bagi pengembang sistem AI maupun platform yang tidak menerapkan langkah-langkah pengamanan yang memadai.

Dari sisi tanggung jawab korporasi, Pasal 118 Undang-Undang Nomor 1 Tahun 2023 tentang KUHP baru memberikan ruang bagi penegakan hukum terhadap badan hukum atau korporasi yang melakukan atau memfasilitasi tindak pidana. Dengan demikian, perusahaan pengembang AI atau penyedia platform media sosial dapat dimintai pertanggungjawaban hukum apabila terbukti lalai atau dengan sengaja membiarkan sistemnya digunakan untuk menyebarkan hoaks. Pendekatan ini sejalan dengan konsep *corporate criminal liability* yang semakin diterapkan dalam hukum modern untuk menghadapi kejahatan berbasis teknologi yang kompleks dan melibatkan banyak pihak. Dalam konteks pembuktian, Peraturan Mahkamah Agung Nomor 4 Tahun 2016 tentang Tata Cara Pemeriksaan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik memberikan pedoman bagi hakim dan penegak hukum dalam menilai alat bukti

elektronik. Namun, tantangan baru muncul karena konten hasil AI sering kali sulit dibedakan dari konten asli. Oleh karena itu, diperlukan penguatan kemampuan *digital forensic* dan sistem verifikasi keaslian data digital agar aparat penegak hukum mampu membedakan antara konten buatan manusia dan hasil rekayasa AI. Tanpa dukungan kapasitas teknis tersebut, penerapan UU ITE dan peraturan lainnya akan sulit menjerat pelaku kejahatan yang memanfaatkan kecanggihan algoritma.

Secara normatif-filosofis, hukum harus menyeimbangkan antara perlindungan terhadap masyarakat dan dukungan terhadap inovasi teknologi. Dalam kasus penyebaran hoaks berbasis AI, prinsip "shared responsibility" perlu diterapkan, di mana tanggung jawab dibagi antara individu pengguna, pengembang sistem, dan penyedia platform. Pemerintah juga perlu memperkuat peran Badan Siber dan Sandi Negara (BSSN) sebagai lembaga pengawas keamanan siber, serta mempercepat penyusunan Rancangan Undang-Undang Kecerdasan Buatan (RUU AI) yang hingga kini masih dalam tahap wacana. RUU tersebut diharapkan dapat mengatur etika penggunaan AI, kewajiban transparansi algoritma, dan mekanisme sanksi bagi pihak yang menyalahgunakan teknologi untuk kepentingan destruktif.

Dengan demikian, analisis yuridis menunjukkan bahwa kejahatan AI di media sosial telah menimbulkan persoalan hukum baru yang tidak dapat sepenuhnya dijawab oleh regulasi yang ada. UU ITE, KUHP, dan UU PDP memberikan dasar awal, namun belum mampu mengakomodasi seluruh kompleksitas AI yang bersifat otonom dan non-manusiawi. Diperlukan pembaruan hukum yang lebih adaptif, penguatan kapasitas teknis aparat penegak hukum, serta pembentukan regulasi khusus terkait kecerdasan buatan. Upaya ini penting agar hukum Indonesia tidak tertinggal dalam menghadapi tantangan era digital dan mampu menegakkan keadilan di tengah kemajuan teknologi yang terus berkembang.

D. Kelemahan dan Kekosongan Hukum

Meskipun Indonesia memiliki beberapa regulasi yang dapat menjerat penyebaran hoaks dan manipulasi opini publik di media sosial, seperti UU ITE (Pasal 28 ayat 1 dan 2), KUHP Pasal 55 dan 56, serta UU PDP (Pasal 65-66), penerapannya dalam kasus kejahatan berbasis AI masih menghadapi kendala signifikan. Salah satu kelemahan utama adalah kurangnya ketentuan spesifik yang mengatur tanggung jawab terhadap teknologi AI yang bersifat otonom dan mampu menghasilkan konten tanpa intervensi manusia langsung. Dengan kata lain, hukum saat ini masih berfokus pada pelaku manusia (*human actor*), sementara AI sebagai pelaku non-manusia tidak

diakui secara eksplisit, sehingga menimbulkan kekosongan hukum dalam hal pembuktian dan pertanggungjawaban.

UU ITE, misalnya, mensyaratkan unsur kesengajaan (*mens rea*) dalam penyebaran berita bohong atau konten menyesatkan. Namun, dalam praktik, AI dapat menghasilkan konten secara otomatis melalui algoritma, sehingga sulit membuktikan niat pelaku manusia di balik sistem. Hal ini membuka celah bagi penyalahgunaan teknologi tanpa konsekuensi hukum yang jelas. Demikian pula, KUHP mengatur pertanggungjawaban melalui konsep penyertaan atau peran serta (*deelneming*), tetapi belum menyesuaikan diri dengan karakter kejahatan digital yang melibatkan pihak ketiga, algoritma, atau sistem otomatis yang memicu kerugian.

UU PDP yang mengatur keamanan dan perlindungan data pribadi juga menghadapi keterbatasan dalam konteks AI. Sistem AI dapat memanipulasi data pribadi atau meniru identitas seseorang (*deepfake*) tanpa pelanggaran langsung terhadap pengendali data, sehingga tanggung jawab hukum menjadi kabur. Sementara itu, mekanisme pengawasan yang ada di BSSN maupun pedoman peraturan perundang-undangan belum mengatur secara rinci standar etika, transparansi algoritma, atau kewajiban mitigasi risiko penyalahgunaan AI. Kekosongan ini menimbulkan risiko hukum bagi masyarakat dan kesulitan aparat dalam menindak pelanggaran secara efektif. Selain itu, belum adanya regulasi khusus tentang AI atau Rancangan Undang-Undang Kecerdasan Buatan (RUU AI) menyebabkan hukum Indonesia belum adaptif terhadap kemajuan teknologi digital. Tidak adanya aturan yang mengatur pertanggungjawaban pengembang, penyedia platform, maupun pengguna AI secara terintegrasi membuat penyalahgunaan AI untuk menyebarkan hoaks atau memanipulasi opini publik cenderung sulit dicegah. Hal ini berbeda dengan beberapa negara yang telah mengatur AI secara spesifik, termasuk kewajiban audit algoritma, transparansi data, dan mekanisme penanganan konten otomatis.

Selain aspek hukum substantif, kelemahan juga terlihat pada kapasitas teknis aparat penegak hukum. Penegakan UU ITE atau UU PDP terhadap konten AI membutuhkan bukti digital yang kompleks, seperti analisis algoritma atau verifikasi keaslian konten *deepfake*. Tanpa peningkatan kemampuan forensik digital, aparat hukum kesulitan membedakan konten buatan AI dengan konten asli yang dihasilkan manusia. Hal ini memperlemah efektivitas peraturan yang ada, meskipun secara normatif sudah memadai untuk kasus hoaks atau manipulasi konvensional. Dengan demikian, dapat disimpulkan bahwa kelemahan dan kekosongan

hukum di Indonesia terkait kejahatan AI terutama berada pada tiga aspek utama: (1) kekosongan regulasi spesifik mengenai AI dan tanggung jawab non-manusia, (2) kesulitan pembuktian kesengajaan pelaku manusia di balik AI, dan (3) keterbatasan kapasitas teknis aparat dalam menegakkan hukum siber modern. Kondisi ini menunjukkan perlunya pembaruan regulasi, baik melalui RUU AI maupun revisi UU ITE dan UU PDP, serta penguatan kolaborasi lintas sektor antara pemerintah, pengembang teknologi, dan masyarakat untuk menciptakan ekosistem digital yang aman dan beretika.

E. Contoh Kasus Penyebaran Berita Hoax Berbasis AI Dimasa Demo : Studi Kasus: Hoaks Video "DPR Temui Mahasiswa Saat Demo Agustus 2025" (Rekayasa AI)

1. Kronologi Kejadian

   Pada Kamis, 28 Agustus 2025, akun Facebook bernama "Mak Sadri" mengunggah sebuah video berdurasi 1 menit 43 detik yang disertai narasi provokatif. Narasi dalam unggahan tersebut berbunyi:

   "DPR meminta Mahasiswa untuk Menghentikan Demo Karena DPR tak bisa dibubarkan. Maka Mahasiswa akan membubarkan DPR. DPR memberanikan diri menemui Mahasiswa, untuk menghentikan demonya, karena DPR tak bisa dibubarkan walaupun Presiden akan membubarkannya tetap tak akan bisa, maka Mahasiswa akan membubarkan DPR secara paksa. Ayo dukung Mahasiswa!"

   Video tersebut menampilkan sekelompok orang beratribut mahasiswa yang tampak melakukan aksi di depan Gedung DPR RI, dengan beberapa tokoh mirip anggota DPR tampak menemui massa. Spanduk di latar belakang berganti-ganti menampilkan tulisan seperti "BUBARKAN DPR", "BUBIRKAN", dan "BUBAKAN", yang tampak tidak konsisten secara visual. Unggahan ini dengan cepat viral di media sosial, terutama Facebook dan WhatsApp, dan mendapat ribuan komentar serta dibagikan ratusan kali dalam waktu kurang dari 12 jam.

2. Klarifikasi dan Penelusuran Fakta

   Tim Pemeriksa Fakta Masyarakat Anti Fitnah Indonesia (Mafindo) melalui platform TurnBackHoax.id segera melakukan pemeriksaan terhadap unggahan tersebut. Mereka menelusuri tangkapan layar video menggunakan Google Lens, yang mengarah ke kanal YouTube "CALNJUTAW4N".Video asli di kanal tersebut diunggah pada Selasa, 26 Agustus 2025, dua hari sebelum unggahan viral di Facebook. Dalam deskripsi video YouTube tersebut, pengunggah dengan jelas menulis

bahwa konten tersebut adalah hasil eksperimen kecerdasan buatan (Artificial Intelligence/AI). Disebutkan bahwa seluruh karakter, objek, dan tempat dalam video merupakan hasil fiktif dan tidak menggambarkan kejadian nyata. Spanduk dan elemen visual lainnya dihasilkan oleh sistem AI berbasis *generative model* yang bekerja secara otomatis, tanpa menggunakan rekaman dunia nyata.

3. Pemeriksaan Teknis dan Pembuktian

Untuk memastikan keaslian konten, tim Mafindo melakukan uji autentikasi menggunakan alat pendeteksi AI "Hive Moderation", sebuah sistem analisis berbasis *machine learning* yang digunakan secara global untuk mendeteksi konten. Hasil pemeriksaan menunjukkan bahwa video tersebut merupakan hasil rekayasa AI dengan probabilitas 99,7%, artinya kemungkinan besar seluruh visual dan karakter dalam video diciptakan secara digital. Analisis lebih lanjut menemukan sejumlah indikator visual khas hasil AI, antara lain:

a. Ketidaksesuaian gerakan bibir dan suara tokoh (unsur *lip-sync mismatch*).
b. Distorsi kecil pada wajah dan gerakan tangan.
c. Ketidak konsistenan latar belakang (spanduk berubah-ubah).
d. Tidak adanya metadata asli (tanggal, lokasi, atau perangkat perekam) pada file video.

Bukti-bukti ini memperkuat kesimpulan bahwa video tersebut adalah konten palsu (fabricated content) hasil teknologi AI generatif.

4. Dampak Sosial dan Potensi Gangguan Publik

Setelah video beredar luas, sejumlah akun anonim memanfaatkannya untuk memicu narasi provokatif di berbagai platform media sosial. Tagar seperti #BubarkanDPR dan #AksiMahasiswa2025 sempat menjadi tren lokal di facebook selama dua hari berturut-turut. Kementerian Komunikasi dan Digital (Komdigi) kemudian mengeluarkan imbauan resmi agar masyarakat tidak mempercayai konten visual yang belum diverifikasi, serta memperingatkan bahaya "AI Hoax Amplification", yaitu peningkatan penyebaran hoaks akibat kemudahan produksi konten palsu menggunakan AI.

Kasus ini menunjukkan bahwa AI dapat digunakan untuk menciptakan realitas buatan yang sangat meyakinkan secara visual, sehingga berpotensi memicu keresahan publik, terutama di tengah situasi

sosial-politik yang sedang memanas seperti masa demonstrasi mahasiswa.

5. Analisis Yuridis

Secara hukum, penyebaran video tersebut dapat dijerat melalui beberapa ketentuan:

a. Pasal 28 ayat (1) UU ITE: larangan penyebaran berita bohong dan menyesatkan yang menimbulkan kerugian masyarakat.
b. Pasal 35 UU ITE: larangan manipulasi informasi elektronik untuk menimbulkan seolah-olah data tersebut otentik.
c. Pasal 55 dan 56 KUHP: pertanggungjawaban bagi pihak yang turut membantu atau menyuruh melakukan tindak pidana.
d. Pasal 66 UU PDP Tahun 2022: kewajiban pengendali data untuk mencegah penyalahgunaan teknologi yang dapat merugikan subjek data pribadi.

Namun, dari aspek pembuktian, kesulitan muncul karena AI sebagai sistem otomatis belum diakui sebagai subjek hukum. Dengan demikian, tanggung jawab hukum lebih diarahkan kepada individu atau kelompok yang mengunggah dan menyebarkan konten, bukan pengembang sistem AI itu sendiri.

Kasus ini juga memperlihatkan kekosongan hukum spesifik terkait rekayasa visual berbasis AI (deepfake dan synthetic media) yang belum secara eksplisit diatur dalam UU ITE maupun KUHP. Maka, regulasi tambahan seperti Rancangan Undang-Undang Kecerdasan Buatan (RUU AI) menjadi sangat mendesak untuk mengisi kekosongan hukum ini.

KESIMPULAN

Berdasarkan analisis yuridis terhadap kasus penyebaran hoaks berbasis kecerdasan buatan (AI) di media sosial, dapat disimpulkan bahwa tanggung jawab hukum dalam hukum positif Indonesia saat ini masih berfokus pada pelaku manusia sebagai subjek hukum utama, sementara AI dan sistem pengembangannya belum diakui secara yuridis sebagai entitas yang dapat dimintai pertanggungjawaban. Pelaku penyebar konten tetap dapat dijerat melalui UU ITE Pasal 28 dan 35, serta KUHP Pasal 55–56, karena secara aktif menyebarkan atau memfasilitasi informasi bohong. Platform media sosial memiliki tanggung jawab etik dan administratif untuk melakukan moderasi serta mencegah penyebaran konten palsu sesuai prinsip due diligence dan ketentuan pengawasan digital dalam UU ITE dan UU PDP 2022. Sementara itu, pengembang AI belum memiliki tanggung jawab hukum langsung,

namun secara moral dan kebijakan publik perlu diatur dalam regulasi khusus seperti RUU Kecerdasan Buatan guna memastikan akuntabilitas, transparansi algoritma, dan keamanan penggunaan AI. Dengan demikian, sistem hukum Indonesia masih memerlukan pembaruan regulatif dan teknis agar mampu menanggapi tantangan baru dalam penegakan hukum siber di era kecerdasan buatan. Kasus hoaks video "DPR Temui Mahasiswa" menjadi contoh nyata penyalahgunaan teknologi AI generatif untuk menciptakan konten palsu yang dapat menghasut opini publik. Hasil verifikasi teknis oleh Mafindo dan Hive Moderation membuktikan bahwa video tersebut tidak merepresentasikan peristiwa nyata, melainkan produk imajinatif yang sepenuhnya dihasilkan oleh AI. Fenomena ini menegaskan bahwa perkembangan teknologi tanpa pengawasan hukum yang memadai dapat mengancam stabilitas sosial dan kepercayaan publik terhadap informasi digital. Oleh karena itu, diperlukan penguatan regulasi hukum siber, peningkatan literasi digital masyarakat, serta pembentukan mekanisme verifikasi konten berbasis AI sebagai langkah preventif terhadap maraknya kejahatan informasi di era kecerdasan buatan.

Saran bagi Pemerintah dan Legislator dalam hal diperlukan penyusunan regulasi khusus seperti Rancangan Undang-Undang Kecerdasan Buatan (RUU AI) yang mengatur aspek pertanggungjawaban hukum, etika penggunaan, dan pengawasan teknologi AI di ruang digital. Pemerintah juga perlu memperkuat koordinasi antar lembaga, terutama Kominfo, BSSN, dan aparat penegak hukum, dalam mendeteksi serta menindak penyebaran konten hasil rekayasa AI. Kemudian bagi Platform Media Sosial untuk meningkatkan sistem moderasi konten berbasis AI yang transparan dan akuntabel, serta memperluas kerja sama dengan lembaga pemeriksa fakta seperti Mafindo untuk menangkal hoaks. Platform wajib menerapkan prinsip due diligence dengan menyediakan fitur verifikasi dan pelaporan konten hasil rekayasa digital. Terakhir bagi Masyarakat diharapkan meningkatkan literasi digital dan kesadaran hukum, dengan selalu memverifikasi informasi sebelum menyebarkannya. Sikap kritis terhadap konten digital, terutama yang menimbulkan provokasi atau isu politik sensitif, merupakan langkah penting dalam mencegah dampak negatif penyebaran hoaks berbasis AI.

DAFTAR PUSTAKA

UNDANG-UNDANG

Indonesia, Republik. 2002. *UNDANG-UNDANG RI NOMOR 3 TAHUN 2002 TENTANG PERTAHANAN NEGARA*. Indonesia.

BUKU

Tümtaş, Mim Sertaç, and Yosra JARRAR. 2022. *International Symposium on*

Strategic and Social Research Full Text Book.

JURNAL

Anggraeny, Kurnia Dewi, Mufti Khakim, and Muhammad Rizal Sirojudin. 2025. "The Urgency of Cybercrime Law Reform in Indonesia : Resolving Artificial Intelligence Criminal Liability." *JUSTISI* 11(1):111–26.

Br, Wahyudi. 2025. "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI." *INNOVATIVE: Journal Of Social Science Research* 5(1).

Gunawan Widjaja, "DEEPFAKE dan Masa Depan Kebenaran: Implikasi Etis dan Sosial," *Berajah Journal* 5, no. 2 (2024): 1–10.

Izdihar, Bilqist. 2024. "Cyberlaw as a Tool to Control the Spread of Hoaxes on Social Media." *Jurnal Hukum Mimbar Justitia (JHMJ)* 10(2):211–22.

Laza, Jeremiah Maximillian, and Rizky Karo Karo. 2023. "PERLINDUNGAN HUKUM TERHADAP ARTIFICIAL INTELLEGENCE DALAM ASPEK PENYALAHGUNAAN DEEPFAKE TECHNOLOGY PADA PERSPEKTIF UU PDP DAN GDPR." *LEX PROSPICIT* 1(2).

Najla Amaly dan Armiah Armiah, "Peran Kompetensi Literasi Digital Terhadap Konten Hoaks dalam Media Sosial," *Alhadharah: Jurnal Ilmu Dakwah* 20, no. 2 (2022): 210–225.

Nurdin, Sri Wahyuni, and Imam Fadhil Nugraha. 2025. "ANCAMAN DEEPFAKE DAN DISINFORMASI BERBASIS AI: IMPLIKASI TERHADAP KEAMANAN SIBER DAN STABILITAS NASIONAL INDONESIA." *JIMR: Journal Of International Multidisciplinary Research* 4(01):73–92.

Pramono, Budi, and Lukman Yudho Prakoso. 2022. "Antisipasi Pertahanan Dan Keamanan Cyberpolitics Dengan Artificial Intelligence." *Jurnal Review Politik* 12(2):196–210.

Purwadi, Ari, and Cita Yustisia Serfiyani. 2022. "Legal Landscape on National Cybersecurity Capacity in Combating Cyberterrorism Using Deep Fake Technology in Indonesia." *International Journal of Cyber Criminology* 16(1):123–40. doi: 10.5281/zenodo.4766560.

Raisa Safina, Khalda Alifia Azzahra, dan Ananda Fersa Dharmawan, "Kajian Yuridis Penggunaan Kecerdasan Artifisial pada Pembuatan dan Penyebaran Konten Pornografi di Media Sosial dalam Hukum Positif Indonesia," *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora* 2, no. 1 (2023/2024): 45–60.

Rendi Syaputra Nur Haida dan Eko Nuriyatman, "Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake melalui Artificial Intelligence (AI) dari Perspektif Hukum Pidana Indonesia," *Jurnal Hukum Respublica* 24, no. 1 (2024): 77–91.

Respati, Adnasohn Aqilla. 2024. "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation." *Jurnal USM Law Review* 7(3):4–12.

Septiawan, Riski. 2024. "CRITICAL ANALYSIS OF AI-PRODUCED MEDIA: A STUDY OF THE IMPLICATIONS OF DEEPFAKE TECHNOLOGY." *DEVOTION Journal of Research and Community Service* 5(7):735–41.

Silalahi, Wilma, Meily Natassya, and Shane Evelina. 2024. "Penggunaan Deepfake Terkait Penyebaran Isu Hoaks Pada Masa Kampanye Pemilu 2024." *Jurnal Bawaslu Provinsi Kepulauan Riau* 6(1):30–45.

Sri Wahyuni Nurdin dan Imam Fadhil Nugraha, "Ancaman Deepfake dan Disinformasi Berbasis AI: Implikasi terhadap Keamanan Siber dan Stabilitas Nasional Indonesia," *JIMR: Journal Of International Multidisciplinary Research* 4, no. 1 (2025): 15–27.

WEBSITE

Kanal YouTube "CALNJUTAW4N," diakses 26 Agustus 2025, https://www.youtube.com/shorts/Zd7S-WTFvqI.

Akun Facebook "Mak Sadri," unggahan video 28 Agustus 2025, https://web.facebook.com/reel/1469743720739263

Hive Moderation, "AI-Generated Content Detection Tool," diakses 28 Agustus 2025, https://hivemoderation.com/ai-generated-content-detection

Anggraeny, Kurnia Dewi, Mufti Khakim, and Muhammad Rizal Sirojudin, 'The Urgency of Cybercrime Law Reform in Indonesia : Resolving Artificial Intelligence Criminal Liability', *JUSTISI*, 11.1 (2025), 111–26

Br, Wahyudi, 'Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI', *INNOVATIVE: Journal Of Social Science Research*, 5.1 (2025)

Indonesia, Republik, *UNDANG-UNDANG RI NOMOR 3 TAHUN 2002 TENTANG PERTAHANAN NEGARA* (Indonesia, 2002)

Izdihar, Bilqist, 'Cyberlaw as a Tool to Control the Spread of Hoaxes on Social Media', *Jurnal Hukum Mimbar Justitia (JHMJ)*, 10.2 (2024), 211–22

Larasati, Anissa, 'Perlindungan Hukum Anak Dalam Penggunaan Media Sosial: Mendesak Penguatan Regulasi Pembatasan Usia Di Indonesia', *MARINews*, 2025 <https://marinews.mahkamahagung.go.id/artikel/perlindungan-hukum-anak-dalam-penggunaan-media-sosial-07j>

Laza, Jeremiah Maximillian, and Rizky Karo Karo, 'PERLINDUNGAN HUKUM TERHADAP ARTIFICIAL INTELLEGENCE DALAM ASPEK PENYALAHGUNAAN DEEPFAKE TECHNOLOGY PADA PERSPEKTIF UU PDP DAN GDPR', *LEX PROSPICIT*, 1.2 (2023)

Nurdin, Sri Wahyuni, and Imam Fadhil Nugraha, 'ANCAMAN DEEPFAKE DAN DISINFORMASI BERBASIS AI: IMPLIKASI TERHADAP KEAMANAN SIBER DAN STABILITAS NASIONAL INDONESIA', *JIMR: Journal Of International Multidisciplinary Research*, 4.01 (2025), 73–92

Pramono, Budi, and Lukman Yudho Prakoso, 'Antisipasi Pertahanan Dan Keamanan Cyberpolitics Dengan Artificial Intelligence', *Jurnal Review Politik*, 12.2 (2022), 196–210

Purwadi, Ari, and Cita Yustisia Serfiyani, 'Legal Landscape on National Cybersecurity Capacity in Combating Cyberterrorism Using Deep Fake Technology in Indonesia', *International Journal of Cyber Criminology*, 16.1 (2022), 123–40 <https://doi.org/10.5281/zenodo.4766560>

Respati, Adnasohn Aqilla, 'Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation', *Jurnal USM Law Review*, 7.3 (2024), 4–12

Septiawan, Riski, 'CRITICAL ANALYSIS OF AI-PRODUCED MEDIA: A STUDY OF THE IMPLICATIONS OF DEEPFAKE TECHNOLOGY', *DEVOTION Journal of Research and Community Service*, 5.7 (2024), 735–41

Silalahi, Wilma, Meily Natassya, and Shane Evelina, 'Penggunaan Deepfake Terkait Penyebaran Isu Hoaks Pada Masa Kampanye Pemilu 2024', *Jurnal Bawaslu Provinsi Kepulauan Riau*, 6.1 (2024), 30–45

Tümtaş, Mim Sertaç, and Yosra JARRAR, *International Symposium on Strategic and Social Research Full Text Book*, 2022

Vidi, Adyaksa, 'Hoaks Pakai Teknologi Deepfake Makin Marak, Masyarakat Dituntut Jeli Cerna Informasi', *Liputan 6*, 2025 <https://www.liputan6.com/cek-fakta/read/6178364/hoaks-pakai-teknologi-deepfake-makin-marak-masyarakat-dituntut-jeli-cerna-informasi>