JIMR: Journal Of International Multidisciplinary Research

http://azramedia-indonesia.azramediaindonesia.com/index.php/JIMR/index
DOI : https://doi.org/10.62668/jimr.v4i01.1551
Email : info@azramediaindonesia.com

Open Access

ANCAMAN *DEEPFAKE* DAN DISINFORMASI BERBASIS AI: IMPLIKASI TERHADAP KEAMANAN SIBER DAN STABILITAS NASIONAL INDONESIA

Sri Wahyuni Nurdin[*1], Imam Fadhil Nugraha[2]
Universitas Hasanuddin, Indonesia
Corresponding Author: sriwahyuninurdin14@gmail.com

Info Article
Received :
01 April 2025
Revised :
04 May 2025
Accepted :
02 June 2025
Publication :
30 June 2025

Keywords:
Deepfake, AI-Based Disinformation, National Security
Kata Kunci:
Deepfake, Disinformasi Berbasis AI, Keamanan Nasional

Abstract: *The development of artificial intelligence (AI), particularly deepfake technology, has posed a serious threat to Indonesia's national security. Deepfakes enable the creation of highly realistic yet fabricated audio-visual content, which can disseminate disinformation, manipulate public opinion, and generate systemic uncertainty within society. In the context of Indonesia, with high internet penetration but low levels of digital literacy, this phenomenon amplifies the risks to institutional legitimacy, democratic processes, and social cohesion. This study employs a qualitative descriptive-narrative approach through literature review and thematic analysis to examine the dynamics of this threat. The findings indicate that AI-based disinformation is not merely a technical issue, but also a psychological, political, and structural one. Addressing this challenge requires regulatory reform, strengthened digital forensic capabilities, and broad-based digital literacy improvement. Without a comprehensive and adaptive response, deepfake disinformation may evolve into an effective tool of destabilization in the era of modern information warfare.*

Abstrak: Perkembangan kecerdasan buatan (artificial intelligence/AI), khususnya teknologi deepfake, telah menjadi ancaman serius bagi keamanan nasional Indonesia. Deepfake memungkinkan pembuatan konten audio-visual yang sangat realistis namun dibuat-buat, yang dapat menyebarkan disinformasi, memanipulasi opini publik, dan menimbulkan ketidakpastian sistemik di masyarakat. Dalam konteks Indonesia, dengan penetrasi internet yang tinggi tetapi tingkat literasi digital yang rendah, fenomena ini memperbesar risiko terhadap legitimasi kelembagaan, proses demokrasi, dan kohesi sosial. Penelitian ini menggunakan pendekatan deskriptif-naratif kualitatif melalui tinjauan literatur dan analisis tematik untuk mengkaji dinamika ancaman ini. Temuan penelitian menunjukkan bahwa disinformasi berbasis AI bukan hanya masalah teknis, tetapi juga masalah psikologis, politis, dan struktural. Untuk mengatasi tantangan ini, diperlukan reformasi regulasi, penguatan kemampuan forensik digital, dan peningkatan literasi digital secara luas. Tanpa respons yang komprehensif dan adaptif, disinformasi deepfake dapat berkembang menjadi alat destabilisasi yang efektif di era perang informasi modern.

INTRODUCTION

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*/ AI) telah menjadi salah satu tonggak revolusi digital abad ke-21. Salah satu manifestasi teknologi ini adalah *deepfake,* sebuah teknik manipulasi citra, audio, dan video yang sangat realistis dengan menggunakan algoritma pembelajaran mendalam (*deep learning*) (Kristiyenda & et al, 2025, p. 150). Meski memiliki potensi positif dalam bidang hiburan, pendidikan, hingga seni, penggunaan *deepfake* juga menimbulkan ancaman serius, terutama dalam konteks penyebaran disinformasi. Di tengah arus digitalisasi global yang masif, fenomena *deepfake* dan disinformasi berbasiss AI telah menjadi tantangan besar bagi banyak negara, termasuk Indonesia, dalam menjaga stabilitas keamanan nasional.

Indonesia sebagai negara demokrasi dan negara kepulauan dengan populasi lebih dari 270 juta jiwa, memiliki tingkat penggunaan media sosial yang sangat tinggi. Menurut laporan *We Are Social* (2024), terdapat 185,3 juta pengguna internet di Indonesia pada Januari 2024, dengan tingkat penetrasi internet sebesar 66,5% dari total populasi (We Are Social, 2024). Kondisi ini menjadikan publik Indonesia sangat rentan terhadap paparan konten digital, termasuk konten palsu dan manipulatif. Dalam konteks ini, ancaman *deepfake* memperparah tantangan disinformasi yang sudah ada sebelumnya, dengan menciptakan konten yang sulit dibedakan dari kenyataan, sehingga memperbesar potensi gangguan terhadap keamanan, ketertiban, serta kepercayaan publik terhadap institusi negara.

Disinformasi berbasiss AI juga bukan hanya terbatas pada video atau gambar. Bot canggih dan jaringan akun palsu dapat digunakan untuk menyebarluaskan hoaks dan algoritma penyusun narasi palsu, membentuk opini publik palsu, dan mengganggu proses demokratisasi, misalnya pada saat pemilihan umum, dan hal ini semakin sulit dideteksi karena kemampuannya untuk meniru gaya bahasa manusia secara alami dan menyasar kerentanan psikologis publik (Nestia Lianingsih, 2025, p. 6). Serangan semacam ini, yang dikenal dengan istilah information *warfare* (perang informasi), telah menjadi bagian dari taktik geopolitik modern. Negara-negara seperti Amerika Serikat dan negara-negara Eropa telah mengalami langsung bagaimana *deepfake* dan disinformasi bisa digunakan untuk mengintervensi urusan politik domestik mereka. Oleh sebab itu, urgensi untuk memahami dan menanggulangi ancaman ini di Indonesia tidak bisa lagi ditunda.

Dalam kerangka hukum dan regulasi, Indonesia telah mengesahkan beberapa instrumen, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan berbagai peraturan terkait siber. Namun, sebagian besar regulasi yang ada belum secara spesifik mengatur fenomena *deepfake* dan penggunaan AI untuk penyebaran disinformasi. Hal ini menyebabkan adanya kesenjangan regulatif (*regulatory gap*) yang dapat dieksploitasi oleh aktor jahat, baik domestik maupun asing (Judijanto & et al, 2025, pp. 105-106). Di sisi lain, penegakan hukum terhadap kasus *deepfake* juga menghadapi tantangan teknis seperti sulitnya mengidentifikasi sumber asli konten *deepfake*, serta keterbatasan kapasitas forensik digital dalam mendeteksi konten manipulatif tingkat tinggi.

Sebagai negara dengan jumlah penggunaan internet yang sangat besar dan penetrasi media sosial yang luas, Indonesia sangat rentan terhadap penyebaran informasi palsu (Zahro, 2024, p. 402). Sementara itu, secara sosial dan budaya, publik Indonesia memiliki kecenderungan untuk cepat menyebarkan informasi tanpa melakukan verifikasi (Dhahir & et al, 2024, p. 359). Tingkat literasi digital yang masih rendah di berbagai wilayah memperparah dampak penyebaran disinformasi. Banyak warga yang belum memahami bagaimana konten *deepfake* bekerja, serta tidak memiliki keterampilan untuk mengidentifikasi manipulasi digital tingkat lanjut. Kondisi ini membuat strategi pertahanan terhadap ancaman *deepfake* tidak bisa hanya mengandalkan pendekatan teknis atau hukum semata, melainkan harus dibarengi dengan pendekatan edukatif dan peningkatan literasi digital secara luas.

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence* /AI) telah merevolusi cara manusia berinteraksi, memperoleh informasi, dan membentuk opini. Namun, kemajuan ini juga membawa dampak negatif, terutama dalam bentuk disinformasi berbasiss AI yang semakin canggih dan sulit di deteksi. Salah satu manifestasi paling mengkhawatirkan dari disinformasi ini adalah teknologi *deepfake,* yang mampu menciptakan konten-konten audio-visual palsu yang sangat meyakinkan dan digunakan untuk menyesatkan publik, menyebarkan propaganda serta merusak kredibilitas individu maupun industri. Indonesia sebagai negara dengan populasi digital yang besar dan tingkat literasi media yang belum merata, ancaman ini menjadi sangat krusial karena berpotensi mengganggu stabilitas politik, menciptakan konflik sosial, dan melemahkan kepercayaan publik terhadap pemerintah secara hukum.

Dalam perspektif konstruktivisime, teknologi *deepfake* tidak hanya menciptakan konten palsu, tetapi turut membntuk persepsi sosial terhadap kebenaran melalui

konstruksi makna yang bersifat intersubjektif (Berger & Luckmann, 1966, pp. 1-10). Ketika masyarakat menerima visual manipulatif sebagai kenyataan, maka batas antara faktual dan yang fiktif menjadi kabur, dan hal ini berisiko menggeser kepercayaan kolektif terhadap institusi-insititusi deomkrasi (Pawelec, 2022, pp. 10-15). Meskipun masyarakat sadar bahwa *deepfake* adalah rekayasa, keberadaannya sendiri sudah cukup untuk menimbulkan keraguan luas dan ketidakpastian epistemik (Harris, 2022, pp. 8-9). Hal ini menjadikan ancaman *deepfake* tidak terletak pada kebohongan semata, melainkan pada kemampuannya mengganggu konstruksi sosial atas realitas yang selama ini menjadi dasar stabilitas publik dan legitimasi politik.

Penelitian yang dilakukan oleh Danielle K. Citron dan Robert Chesney dalam artikel *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (2019) memberikan dasar konseptual yang kuat mengenai ancaman serius yang ditimbulkan oleh teknologi *deepfake* dalam konteks demokrasi dan keamanan nasional. Dalam kajiannya, mereka menjelaskan bagaimana perkembangan pesat dalam teknologi kecerdasan buatan, terutama *generative adversarial networks* (GANs), telah memungkinkan pembuatan konten audio-visual palsu yang sangat meyakinkan dan sulit untuk dideteksi (Citron, 2019, pp. 1762-1763). Fenomena ini tidak hanya berdampak pada privasi individu, tetapi juga merusak tatanan sosial-politik dengan memanipulasi wacana publik, menciptakan keraguan terhadadp kebernaran, dan bahkan menurunkan legitimasi lembaga-lembaga negara. Konsep seperti *liar's diviend* yang diangkat dalam studi tersebut menyoroti proses difusi teknologi ini yang tidak hanya beredar di tangan aktor negara, tetapi juga menyebar luas ke aktor non-negara, termasuk individu, kelompok ekstremis, hingga sindikat kriminal yang dapat memanfaatkannya untuk kepentingan ekonomi maupun politik.

Kajian Citron dan Chesney menjadi sangat relevan karena memberikan gambaran teoritis dan empiris mengenai bagaimana disinformasi berbasiss AI terutama dalam bentuk *deepfake* dapat mengganggu stabilitas politik, melemahkan kepercayaan publik, dan menciptakan kerentanan dalam sistem demokrasi, yang juga merupakan isu sentral dalam keamanan nasional Indonesia. Negara berkembang dengan infrastruktur digital yang terus berkembang seperti Indonesia menjadi target potensial dari sosial yang kian menguat. Dengan mengacu pada pemikiran dan temuan Citron dan Chesney, penelitian ini akan menelaah bagaimana narasi dan penyebaran konten deepdake di ruang digital Indobrsia dapat mengancam ketertiban nasional, serta menganalisis respons strategis yang dapat dikembangkan dalam kerangka kebijakan keamanan siber kontemporer.

Kemudian dalam penelitian Vaccari dan Chadwik (2020) memberikan kontribusi dalam memahami dampak politik dari teknologi *deepfake*, khususnya dalam konteks disinformasi dan kepercayaan publik terhadap kepercayaan publik terhadap berita digital. Melalui eksperimen terhadap 2.005 responden di Inggris, mereka mengevaluasi respons individu terhadap video *deepfake* politik yang menampilkan pernyataan palsu dari tokoh publik, serta bagaimana ketidakpastian (*uncertainty*) yang timbul akibat eksposur tersebut memengaruhi tingkat kepercayaan terhadap berita di media sosial (Vaccari & Chadwick, 2020, p. 1). Hasilnya menunjukkan bahwa meskipun tidak semua tertipu oleh *deepfake*, tingkat ketidakpastian meningkat secara signifikan, dan ketidakpastian ini pada gilitannya menyebabkan penurunan kepercayaan terhadap informasi politik media sosial. Temuan ini menekankan bahwa bahaya utama dari *deepfake* bukan hanya kebohongan eksplisit yang disebarkan, tetapi juga kerusakan sistemik terhadap ekosistem informasi digital yang dapat memperkuat sinisme, melemahkan literasi media, dan merusak partisipasi publik yang sehat dalam diskursus politik.

Keterkaitan antara kajian ini dengan penelitian penulis sangatlah erat. Di Indonesia, sebagai negara demokrasi digital yang besar dengan tantangan literasi media yang kompleks, ancaman disinformasi berbasiss AI melalui *deepfake* berpotensi menciptakan ketidakpastian massal di ruang publik dan mengikis kepercayaan terhadap institusi-institusi formal, termasuk pemerintah dan media. Jika ketidakpercayaan ini menyebar luas, hal tersebut dapat menciptakan kondisi yang rentan terhadap instabilitas sosial dan politik. Penelitian penulis yang berfokus pada dampak disinformasi AI terhadap keamanan nasional Indonesia dapat mengambil pelajaran penting dari pendekatan eksperimental Vaccari dan Chadwick, terutama dalam menggarisbawahi peran *deepfake* dalam membentuk persepsi publik, menciptakan disorientasi informasi, serta memengaruhi sikap warga terhadap otoritas dan berita. Artikel ini memperkuat dasar teoritis dan empiris bagi analisiss mengenai bagaimana ancaman *deepfake* bukan hanya teknis, tetapi juga psikologis dan politis yang semuanya berdampak pada stabilitas nasional dan keamanan siber kontemporer.

Ancaman *deepfake* terhadap keamanan nasional telah mendorong negara-negara maju untuk mengembangkan teknologi deteksi otomatis, seperti sistem verifikasi berbasiss AI, serta membentuk kerjasama internasional dalam menghadapi penyebaran konten palsu (T20 INDONESIA, 2022, p. 14). Indonesia juga perlu mengikuti jejak ini dengan mengembangkan kebijakan pertahanan siber yang adaptif, membangun

Kemampuan teknis untuk deteksi dini dan respons cepat terhadap *deepfake*, serta memperkuat kolaborasi antar lembaga baik di tingkat nasional maupun internasional.

Menghadapi fenomena ini, penelitian yang mendalam mengenai ancaman *deepfake* dan disinformasi berbasiss AI terhadap stabilitas keamanan nasionaal Indonesia menjadi sangat penting. Penelitian ini tidak hanya bertujuan untuk mengidentifkasi tingkat ancaman dan dampak potensialnya, tetapi juga untuk menyusun rekomendasi strategis dalam rangka memperkuat ketahanan nasional. Dengan memahami dinamikan ancaman ini secara komprehensif, Indonesia telah dapat lebih siap menghadapi era baru di mana perang informasi berbasiss AI menjadi bagian integral dari tantangan keamanan nasional.

METHOD

Penelitian ini menggunakan pendekatan kualitatif dengan model naratif deskriptif. Pendekatan ini dipilih untuk memahami secara mendalam dan komprehensif bagaimana disinformasi berbasiss kecerdasan buatan, termasuk teknologi *deepfake*, membentuk ancaman nyata terhadap stabilitas keamanan nasional Indonesia. Melalui model naratif deskriptif, penelitian ini berfokus pada konstruksi narasi dan makna yang terbentuk di balik fenomena tersebut, serta dampaknya terhadap persepsi publik, kebijakan negara, dan respons keamanan siber nasional.

Jenis penelitian yang digunakan bersifat deskriptif analitik, dengan tujuan menggambarkan secara rinci dan sistematis fenomena disinformasi dan manipulasi digital. Penelitian ini tidak bertujuan untuk menguji hipotesis, melainkan untuk menyajikan gambaran naratif yang kaya mengenai bagaimana ancaman ini berkembang, siapa aktor-aktornya, dan bagaimana respons institusi terhadapnya. Fokus utama diletakkan pada pemetaan narasi, pola penyebaran informasi, serta interpretasi sosial dan politis terhadap konten *deepfake* dan disinformasi berbasiss AI.

Teknik pengumpulan data dilakukan melalui studi pustaka dan dokumentasi. Data dikumpulkan dari berbagai sumber, termasuk artikel jurnal akademik, laporan resmi dari lembaga nasional, serta laporan organisasi internasional. Selain itu, berita dari, analisis media, dan laporan investigatif, serta transkrip diskusi publik dan wawancara pakar juga digunakan sebagai bahan kajian. Sumber data tersebut mencakup baik data primer tidak langsung maupun data sekunder yang relevan dengan fokus penelitian. Analisiss data dilakukan melalui analisiss tematik naratif. Tahap pertama melibatkan proses koding terbuka untuk mengidentifikasi isu-isu utama dan kata kunci penting dari

seluruh sumber data. Selanjutnya, dilakukan koding aksial untuk menemukan hubungan antar tema yang muncul, seperti hubungan antara penyebaran disinformasi dengan momentum politik atau isu identitas. Terakhir, dilakukan konstruksi naratif yang merangkai berbagai elemen tersebut ke alur cerita atau deskripsi tematik yang dapat menjelaskan dampak disinformasi dan *deepfake* terhadap keamanan nasional secara utuh.

RESULTS AND DISCUSSION

Results

Munculnya teknologi *deepfake* merupakan titik balik dalam dinamika disinformasi global. Teknologi ini memanfaatkan kecerdasan buatan untuk menghasilkan konten sintesis yang menyerupai rekaman video atau suara tokoh publik, namun tidak pernah benar-benar terjadi. Dalam beberapa tahun terakhir, kemampuan *deepfake* berkembang pesat, tidak hanya dari sisi kualitas visual, tetapi juga kemudahan akses oleh publik. Hal ini menandai pergeseran dari ancaman digital berbasiss teks atau gambar ke bentuk baru yang lebih meyakinkan dan sulit dibantah secara visual.

Pada dasarnya, keamanan nasional tidak hanya berkaitan dengan pertahanan militer, tetapi juga mencakup aspek sosial-politik, dan informasi publik. Ketika teknologi dapat menciptakan ketidakpastian secara sistemik seperti melalui disinformasi visual berbasiss AI, maka kemampuan negara untuk menjaga ketertiban sosial dan kestabilan politik dapat terganggu. Jika dilihat dari geopolitik, *deepfake* bisa dipakai oleh aktor negara atau non-negara untuk membuat narasi provokasi, misalnya dengan mengedarkan video artillery misrepresentasi Papua, atau rekayasa audio pejabat BNPB meminta bantuan militer asing di saat krisis. Ini bisa memicu reaksi publik misinformatif dan memaksa pemerintah melakukan manuver terus-menerus untuk klarifikasi. Kondisi seperti ini menggerus kepercayaan publik terhadap negara dan membuka celah bagi destabilisasi internal dan gangguan *soft power.*

Evolusi Teknologi *Deepfake* dan Disinformasi

Manipulasi visual sebagai instrumen politik dan sosial bukanlah fenomena baru. Jauh sebelum *Artificial Intelligence* (AI) hadir, praktik ini sudah digunakan untuk membentuk opini publik. Salah satu contoh paling awal terjadi pada abad 19, di Amerika Serikat, Thomas Nast lewat ilustrasi karikatur tajam berhasil mengungkapkan praktik korupsi, menciptakan simbol politik seperti keledai Demokrat, serta

memperkuat fungsi jurnalistik sebagai pengontrol kekuasaan (Szélpál, 2023). Ini menandakan bahwa sejak awal, representasi visual telah dimanfaatkan sebagai alat persuasi dan propaganda. Namun dititk balik yang revolusioner terjadi pada tahun 2014 ketika Ian Godfellow dan timnya memperkenalkan *Generative Adversial Networks* (GANs). Teknologi ini memungkinkan komputer menciptakan citra dan suara tidak hanya sintetis, tetapi juga sangat meyakinkan secara visual dan auditif. GANs bekerja dengan dua jaringan saraf tiruan yang saling bersaing, satu bertugas menciptakan konten palsu, dan satu lagi bertugas mengenali keasliannya (Goodfellow, et al., 2014, pp. 1-2). Persaingan ini menciptakan hasil semakin realistis dan sulit dibedakan.

Teknologi *deepfake* pertama kali dikenal luas pada tahun 2017 melalui forum daring Reddit, ketika pengguna mengunggah video manipulatif yang menampilkan wajah selebritas terkenal pada tubuh orang lain yang telah disintesis secara digital menggunakan aplikasi *open-source* (Tulga, 2024, pp. 51-52). Sejak saat itu, teknologi ini berkembang cepat yang semula hanya eksperimen terbatas, kini berubah mulai digunakan untuk tujuan yang lebih serius dan politis termasuk untuk tujuan disinformasi. Pascaperkembangan tersebut, *deepfake* mulai memasuki ranah politik global. Salah satu contoh terkenal adalah video mantan presiden Amerika Serikat, Barack Obama yang disintesis oleh komedian Jordan Peele, yang menunjukkan bagaimana kata-kata seorang pemimpin dunia dapat dipalsukan dengan sempurna (Gstalter, 2018).

Kemajuan teknologi kecerdasan buatan telah melahirkan era baru dalam praktik disinformasi, di mana konten manipulatif tidak lagi terbatas pada teks atau gambar statis, melainkan menjelma dalam bentuk audio dan video yang tampak autentik, *deepfake* merupakan produk dari teknologi *generative adversarial networks* (GANSs) yang mampu menciptakan citra dan suara tokoh publik secara sintesis dengan ketepatan yang mengkhawatirkan (Latifa, 2024). Kemudahan akses terhadap perangkat lunak *open-source* menjadikan pembuatan video palsu kini bukan lagi domain ekslusif aktor negara, melainkan juga tersedia bagi publik umum, bahkan kelompok radikal. Di Indoensia, penyebaran video *deepfake* sangat mungkin terjadi di tengah tingginya penggunaan media sosial dan rendahnya literasi digital. Akibatnya, persepsi publik terhadap tokoh atau peristiwa politik dapat dengan mudah dibentuk oleh visualisasi palsu yang tampak nyata dan emosional.

Disinformasi visual seperti *deepfake* bekerja secara lebih dalam dibandingkan bentuk disinformasi konvensional, karena menyerang cara manusia memproses

informasi secara intuitif (Hancock & Bailenson, 2021, pp. 150-151). Ketika seseorang melihat video yang tampak meyakinkan, skeptisisme cenderung melemah karena otak mempersepsikan visual sebagai representasi langsung dari kenyataan. Dengan kata lain, visualisasi manipulatif tidak hanya membingungkan logika, tetapi juga memanfaatkan respons emosional sebagai jalur penyebaran yang efektif (Martel et al., 2020, pp. 2-3). Hal ini menjadikan *deepfake* sebagai alat propaganda digital yang sangat berbahaya, terutama di tengah publik dengan keterbatasan kemampuan verifikasi informasi secara mandiri.

Meskipun video *deepfake* tidak selalu berhasil menipu pemirsanya secara langsung, ancaman utamanya justru terletak pada kemampuannya menciptakan ketidakpastian terhadap kebenaran. Ketika publik tidak yakin apakah suatu video benar atau tidak, maka kepercayaan terhadap media, institusi, dan bahkan realitas digital secara keseluruhan dapat terguncang. Dalam konteks ini, *deepfake* menjadi alat disinformasi yang sangat efektif karena mampu menabur keraguan, bukan sekedar menyebarkan kebohongan. Ketidakpastian ini memunculkan efek domino berupa penurunan kepercayaan terhadap sistem politik, hasil pemilu, dan tokoh publik, yang pada akhirnya berdampak pada stabilitas demokrasi (Pawelec, 2022, pp. 5-7). Hal tersebut menjadi semakin berbahaya ketika aktor-aktor politik justru memanfaatkan eksistensi *deepfake* untuk menyangkal pernyataan otentik dengan mengklaim bahwa bukti yang beredar adalah palsu.

Fenomena tersebut disebut dengan *liar's dividend,* yaitu keuntungan strategis dari adanya teknologi yang memungkinkan pembuat hoaks atau pelaku pelanggaran menyangkal keterlibatan mereka (Pawelec, 2022, p. 5). Dalam konteks penegakan hukum, hal ini menciptakan tantangan baru karena bukti visual yang sebelumnya dianggap kuat bisa diragukan keabsahannya. Bagi Indonesia, ketidakpastian ini menjadi ancaman serius, terutama menjelang momen politik besar seperti pemilu atau saat krisis sosial. Publik yang tidak mampu membedakan informasi yang valid dan mana yang manipulatif akan cenderung bersikap apatis atau mudah diprovoaksi. Dalam jangka panjang, ketidakpastian yang tidak tertanggulangi dapat mengikis kepercayaan publik terhadap seluruh sistem demokrasi dan keamanan negara.

Ketidakpastian sebagai Senjata Informasi

Di era digital kontemporer, strategi disinformasi telah berevolusi dari sekedar penyebaran informasi palsu menjadi bentuk manipulasi yang jauh lebih kompleks, yaitu

menciptakan ketidakpastian sistemik. Ketidakpastian ini bukan sekedar efek samping dari informasi yang keliru, melainkan menjadi inti strategis untuk mengaburkan batas antara yang benar dan yang palsu. Teknologi *deepfake,* dengan kemampuannya menghasilkan video dan audio yang menyerupai kenyataan, memainkan peran penting dalam membangun ekosistem disinformasi yang bersandar pada ambiguitas dan kebingungan publik.

Salah satu ilustrasi utama dari strategi ini adalah model "*firehouse of falsehood*", yaitu teknik propaganda yang menekankan volume besar, kecepatan tinggi, dan distribusi multikanal, dan sering kali tanpa konsistensi logis (Paul & Matthews, 2016, p. 2). Dalam pendekatan ini, tujuan utama bukanlah meyakinkan publik atas suatau narasi, melainkan membanjiri mereka dengan informasi yang saling bertentangan hingga kapasitas kognitif untuk membedakan mana yang benar menjadi tumpul. Ketika di kombinasikan dengan konten *deepfake,* efeknya menjadi semakin destabilisasional: publik tidak hanya dibuat ragu terhadap konten palsu, tetapi juga mempertanyakan kebenaran dari semua konten, termasuk yang otentik.

Ketidakpastian ini menjadi medan subur bagi berkembangnya fenomena *liar devidend,* yakni situasi ketika aktor yang tertuduh dapat menyangkal bukti visual dengan dalih bahwa konten tersebut adalah hasil rekayasa *deepfake* (França, 2022). Dalam studi Daniel Schiff dan timnya dari Georgia Tech dan Emory University pada tahun 2023. Melalui serangkaian eksperimen berbasiss survei, mereka menemukan bahwa politisi yang menghadapi tuduhan melalui video *deepfake* dapat memperoleh peningkatan dukungan ketika mereka menyangkalnya dengan mengklaim bahwa konten tersebut palsu. Penyangkalan tersebut bahkan memberi keuntungan politik yang lumayan besar, berkisar antara +0,17 hingga +0,21 standar deviasi dalam tingkat kepercayaan dan dukungan pemilih terhadap politisi tersebut (Schiff et al., 2025, pp. 75-87). Artinya, publik yang awalanya diharapkan menjadi lebih waspada terhadap disinformasi, justru mejadi semakin permisif pada penyangkalan yang tidak berbasiss bukti.

Dalam lingkungan yang sudah tercemar oleh ketidakpastian sistemik, publik menjadi lebih permisif terhadap kebohongan dan lebih skeptis terhadap kebenaran. Kepercayaan yang rapuh ini menjadi target utama dari aktor-aktor yang ingin melemahkan legitimasi institusi politik, media, dan hukum. Ketidakpastian ini tidak beroperasi dalam ruang kosong. Ia menyusup dalam struktur sosial yang telah lebih dulu memiliki kerentanan seperti rendahnya literasi digital, polarisasi politk, dan

kurangnya kepercayaan publik terhadap lembaga negara. Dalam kondisi ini, disinformasi berbasiss *deepfake* tidak perlu meyakinkan siapa pun. Cukup dengan memantik keraguan, ia telah berhasil menjalankan fungsinya dengan menciptakan kebingungan kolektif dan kelumpuhan epistemik.

Kritik terhadap narasi dominan tentang disinformasi sering kali terlalu fokus pada validitas konten, bukan pada efek jangka panjang dari atmosfer keraguan yang diciptakan. Padahal, dalam arsitektur ancaman siber kontemporer, nilai strategis dari ketidakpastian terletak pada kemampuannya melemahkan fondasi komunikasi publik. Publik yang terus-menerus dihadapkan pada konten yang meragukan akan mengalami *disempowerment*, di mana mereka tidak memiliki alat untuk memverifikasi, tidak percaya pada sumber informasi, dan pada akhirnya memilih untuk tidak peduli. Sikap apatis ini merupakan bentuk keberhasilan paling subtil dari disinformasi bebasis ketidakpastian.

Ketidakpastian ini bukan hanya bentuk ancaman kognitif, tetapi juga politik. Ia mendistorsi hubungan antara rakyat dan negara, karena mengikis dasar kepercayaan yang menjadi perekat demokrasi. Dalam situasi seperti ini, setiap diskursus publik menjadi rentan terhadap dilegitimasi, karena setiap argumen dapat diserang bukan dengan sanggahan substansial, tetapi cukup dengan tuduhan bahwa “itu palsu”. Realitas menjadi relatif, bukan karena berubah, tetapi karena dibuat tampak tak bisa dipercaya. Lebih dari itu, bahkan ketidakpastian bisa dijadikan sebagai senjata informasi menggeser medan perang dari ranah fisik ke ranah persepsi. Tidak perlu lagi menghancurkan infrastruktur untuk melumpuhkan negara cukup goyahkan perspektif kolektif terhadap realitas, dan sistem akan runtuh dari dalam. Inilah bentuk perang informasi modern yang paling berbahaya, ia menyerang kepercayaan sebagai infrastruktur paling mendasar dalam publik.

Implikasi Keamanan Nasional dalam Konteks Indonesia

Indonesia saat ini memiliki penetrasi internet yang sangat tinggi, sebanyak 79,5% penduduk usia 13 tahun keatas sudah masuk ke dalam lingkup online, setara dengan 221 juta pengguna, dengan rata-rata penggunaan harian mencapai 7 jam 28 menit (APJII, 2024). Namun sekaligus, skor literasi hanya berada pada angka 3,5 dari skala indeks 1-5, tergolong rendah dibanding negara tetangga lainnya (INDOPOSCO.Id, 2024). Data ini menunjukkan ekosistem digital kita terdiri dari khalayak yang sangat terpaapr media namun minim pada keterampilan dalam memilah informasi berbasiss

ketidakpastian atau hoaks. Saat disinformasi berbentuk *deepfake* muncul, publik tidak hanya bingung memverifikasi suatu fakta, tetapi juga cenderung menyerah dan beralih pada narasi "ini pasti palsu" yang telah dijelaskan pada strategis *liar's dividend* yang memanfaatkan *low-capacity society* untuk menyebarkan disorientasi.

Menurut survei APJII (2023-2024) 24,7% hoaks yang beredar di platform digital yang bersinanggungan dengan konten politik (Rosy Saptoyo, 2024). Dalam artian hampir satu dari empat klaim palsu secara langsung mencoba mempengaruhi opini publik terkait isu-isu politik. Di tengah persaingan informasi menjelang pemilu atau pilkada, banyak politisi yang menjadi subjek tuduhan skandal dengan hanya perlu membalik narasi dengan menyebutnya "*deepfake* hoaks" dan banyak publik tunduk pada ketidakpastian. Pendekatan ini memerluan klarifikasi mendalam, yaitu dengan cukup menabur keraguan. Sekali publik merasa harus mempertayakan keaslian bukti visual, legitimasi politik dan institusi dapat mudah didismantle.

Teknologi *deepfake* tidak hanya menipu mata dan telinga publik, ia juga menghadirkan ancaman terhadap sistem keamanan data officiel. Studi oleh Arvi Erawan dan timnya pada tahun 2024, memperingatkan bahwa deepfake bisa digunakan untuk mengelabui sistem biometrik seperti e-KTP, sidik jari, dan *voice authentication* (Palindra dkk., 2024, hal. 111-113). Jika data biometrik tidak terlindungi dengan sistem yang kuat dan terenkripsi, negara menghadapi ancaman impersonasi massal, potensi sabotase layanan publik, bahkan identitas palsu dalam sistem pemerintahan. Ancaman ini melebar ke ranah keamanan nasional dengan penyalahgunaan data biometrik oleh pihak asing atau kriminal terorganisir dapat menyebabkan kebocoran gestural keimigrasian, data PNS, data parlemen, dan data negara kehilangan kendali atas sistem identitas digital warganya sendiri.

Pada Juni 2024, terjadi serangan ransomeware LockBit 3.0 terhadap Pusat Data Nasional (PDN) Surabaya, yang mempengaruhi lebih dari 230 instansi pemerintahan, termasuk imigrasi dan bandara kebutuhan untuk membayar tebusan sebesar USD 8 juta membuat publik cemas (Anri Syaiful, 2024). Setelah kejadian ini, data backup dilaporkan tidak cukup ada walaupun pemerintah segera mewajibkan backup terpusat dan zonasi di PDN lainnya. Insiden ini terbukti melumpuhkan layanan publik esensial, menimbulkan antrean panjang dan gangguan di titik perbatasan, serta memantik borrower kepercayaan publik terhadap kapasitas pelayanan digital pemerintah.

Serangan PDN membuka pintu agar platform sosial digunakan sebagai medan proxy *warfare*. Salah satu contoh viral adalah video palsu Presiden Joko Widodo

berbicara Mandarin, sempat memicu spekulasi bahwa ia pro pada China, sebelum Komdigi menegaskan bahwa hal tersebut manipulatif (KOMDIGI, 2023). Media sosial dengan kecenderungan *echo chamber* memperparah dampaknya, di mana publik terbagi antara yang percaya langsung atau yang skeptis tanpa verifikasi. Ketidakpastian ini memicu kondisi *distrust economy*, dimana publik tidak percaya pada media mainstream, tetapi juga tidak yakin narasi alternatif. Akibatnya, demokrasi dirudung oleh kelelahan informasi dan apatisme politik yang terbukti melalui tren penurunan partisipasi PTM dan kepercayaan terhadap lembaga sejak pilpres 2019-2024 yang terus menurun (Komisi Pemilihan Umum Kota Salatiga, 2025).

Ketika kebenaran dipertanyakan melalui taktik *deepfake* dan ketidakpastian sistemik, negara tidak hanya menghadapi kebingungan publik, tetapi juga risiko delegitimasi institusi. Badan pemerintah, media, bahkan proses pemilu menjadi sasaran empuk. Di Indonesia yang multikultural dan terfragmentasi, *deepfake* bisa digunakan untuk menyebarkan narasi palsu tentang suku, agama, ras, dan antargolongan yang tanpa verifikasi dapat memicu konflik horizontal. Dengan kepercayaan publik yang mudah goyah, stabilitas nasional bisa terguncang hanya karena serangan informasi, bukan serangan fisik. Ketika publik mulai meragukan kebenaran atas apa yang mereka lihat atau dengar, maka kredibilias lembaga negara, pemilu, bahkan media pun ikut terancam. Inilah yang disebut sebagai krisis epistemik, yaitu krisis terhadap kepercayaan terhadap kebenaran dan otoritas informasi yang merupakan fondasi dari ketidakstabilan nasional jangka panjang.

Dari sisi legal-formal, indonesia memang sudah memiliki beberapa kerangka hukum yang dapat digunakan untuk menagani penyebaran konten manipulatif. UU No.19 Tahun 2016 Informasi dan Transaksi Elektronik (UU ITE) Pasal 45A ayat (1) mengatur penyebaran berita bohong yang menyesatkan ruang digital, dengan ancaman pidana maksimal 6 tahun dan denda Rp1 miliar (Republik Indonesia, 2016). Selain itu, Undang-undang Perlindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 juga memberi payung hukum terhadap penyaahgunaan data biometrik yang kerap digunakan dalam pembuatan *deepfake* (Presiden Republik Indonesia, 2022).

Namun demikian, peraturan-peraturan tersebut masih memiliki celah yang besar. Tidak ada satupun undang-undang yang secara eksplisit mendefinisikan dan mengatur "*deepfake*" sebagai istilah hukum. Hal ini membuat proses penegakan hukum harus menafsirkan pasal-pasal umum dalam hal teknologi yang sangat spesifik. Selain itu, penindakan terhadap konten *deepfake* membutuhkan keahlian teknis digital forensik

yang belum merata di seluruh lembaga hukum. Akibatnya, efek disinformasi sudah terjadi, sementara proses hukum baru dimulai, yang mana hal ini menimbulkan efek terlambat yang bisa dimanfaatkan aktor-aktor politik secara strategis.

Krisis ini mengindikasikan bahwa negara belum cukup siap menghadapi dimensi "perang informasi" yang sangat kompleks dewasa ini. Tidak seperti perang konvensional, serangan *deepfake* bersifat asimetris, tidak selalu dilakukan oleh negara lain, tetapi bisa dilakukan oleh kelompok radikal, partisian politik domestik, bahkan aktor individu yang memiliki akses pada teknologi. Dengan demikian, pendekatan pertahanan negara tidak hanya bersifat militeristik, tetapi juga harus diperluas ke aspek literasi digital, penguatan kapasitas siber, dan reformasi regulasi. Pemerintah perlu mempertimbangkan pembuatan undang-undang khusus yang mengatur produksi, distribusi, dan penggunaan konten sintetis,

Situasi ini juga menyoroti perlunya pembaruan sistem pendidikan hukum, media, dan digital *citizenship*. Literasi digital bukan hanya soal mengajari publik cara menggunakan teknologi, tetapi juga membekali mereka kemampuan untuk mendeteksi, menganalisis, dan mengevaluasi informasi secara kritis. Ketika publik tidak memiliki kemampuan untuk membedakan kebenaran dan manipualasi, maka demokrasi menjadi sangat rentan terhadap disinformasi. Tanpa kemampuan publik untuk melakukan verifikasi secara mandiri, setiap kebohongan bisa menjadi kebenaran yang dipercaya secara luas (Mirsky & Lee, 2020, pp. 1-3).

Ketidak mampuan negara untuk mengelola ancaman disinformasi berbasiss AI menunjukkan adanya kekosongan dalam kebijakan keamanan nasional yang menyeluruh. Ketika aktor-aktor politik bisa memanfaatkan teknologi *deepfake* untuk menyangkal kebenaran, memperkuat basis politiknya, atau bahkan menjatuhkan lawan melalui manipulasi visual, maka proses demokrasi tidak lagi sehat dan adil. Sebaliknya, ia menjadi panggung manipulatif yang mempermainkan persepsi rakyat. Hal ini tidak hanya berbahaya bagi demokrasi, tetapi juga memperbesar risiko konflik sosial yang bisa meluas menjadi instabilitas nasional.

Dalam menghadapi ancaman *deepfake* dan disinformasi berbasiss kecerdasan buatan, strategi nasional yang komprehensif menjadi keharusan guna menjaga stabilitas kemanan dan ketahanan informasi Indonesia. Langkah pertama yang perlu dilakukan adalah memperkuat kerangka regulasi yang adaptif terhadap dinamika teknologi, dengan menambahkan klausul spesifik dalam Undang-Undang ITE maupun peraturan turunan lainnya terkait produksi dan distribusi konten manipulatif berbasis AI. Selain

itu, peningkatan kapasitas teknis melalui pengembangan sistem deteksi otomatis dan teknologi forensik digital berbasis AI sangat penting, terutaa bagi lembaga strategis berbasiss BSSN san Kominfo. Upaya ini harus dibarengi dengan literasi digital yang terstruktur dan menyeluruh, karena aspek kognitif masyarakat menjadi faktor penentu dalam menahan laju penyebaran informasi palsu

Masyarakat yang memahami bagaimana konten *deepfake* diproduksi serta mampu mengenali ciri-cirinya akan lebih resisten terhadap manipulasi digital. Di sisi lain, kerjasama internasional juga perlu diperkuat, mengingat sifat lintas batas dari disinformasi digital. Indonesia perlu bergabung dalam koalisi global yang fokus pada keamanan siber dan etika AI untuk mempercepat pertukaran data, teknologi, serta pengalaman dalam menangkal ancaman serupa. Akhirnya, pembangunan ekosistem kepercayaan menjadi fondasi jangka panjang, termasuk melalui penggunaan teknologi autentikasi konten resmi, verifikasi independen, dan penguatan transparansi informasi publik. Strategi ini bukan hanya reaktif terhadap ancaman, tetapi juga bersifat preventif dan transformatif demi menjadi integritas demokrasi di era informasi.

Dampak Sosial dan Politik dari *Deepfake* terhadap Indonesia

Deepfake memiliki potensi merusak tatanan demokrasi melalui tiga jalur utama; 1) manipulasi persepsi pemilih, 2) pelemahan lembaga publik, dan 3) polarisasi sosial. Pertama dalam hal pemilu, video *deepfake* dapat digunakan untuk menyerang kredibilitas kandidat politik dengan menyebarkan rekaman palsu yang memperlihatkan perila ku tercela atau ucapan yang tidak pernah mereka katakan. Dalam kondisi menjelang pemilihan umum, konten semacam ini bisa menyebar dengan cepat dan memengaruhi pemilih yang belum menentukan pilihan. Meskipun kemudian dibantah atau melakukan klarifikasi, kerusakan persepsi yang terjadi bisa bersifat permanen karena sifat informasi palsu yang lebih cepat melekat.

Deepfake dapat melemahkan kepercayaan terhadap lembaga demokrasi seperti Komisi Pemilihan Umum (KPU), Mahkamah Konstitusi, bahkan kepolisian. Jika beredar video yang tampak otentik namun palsu, misalnya menampilkan petugas pemilu sedang melakukan kecurangan, maka publik bisa kehilangan kepercayaan terhadap proses demokrasi itu sendiri. Lembaga-lembaga ini akan menghadapi tantangan dalam mempertahankan integritasnya di mata publik karena video *deepfake* sering kali menyentuh aspek visual dan emosional yang sulit didekonstruksi melalui klarifikasi rasional.

Deepfake berpotensi memperdalam polarisasi sosial. Konten palsu yang menargetkan kelompok etnis, agama, atau politik tertentu dapat digunakan untuk menyulut kebencian, meningkatkan permusuhan, dan memicu kekerasan. Indonesia sebagai negara dengan keragaman yang tinggi sangat rentan terhadap jenis disinformasi yang bersifat memecah belah. Jika tidak ditangani dengan baik, penggunaan *deepfake* dapat menciptakan efek disinformasi berantai yang memperparah fragmentasi sosial dan melemahkan kohesi nasional. Demokrasi yang sehat membutuhkan ruang publik yang dapat dipercaya, karena *deepfake* dapat merusak fondasi tersebut dari dalam.

CONCLUSION

Penelitian ini menyimpulkan bahwa penggunaan teknologi berbasiss *Artificial Intelligence* selain memberikan keuntungan dalam aspek-aspek pertumbuhan negara, dapat menjadi sebuah ancaman terutama terhadap negara-negara yang masih berkembang mulai dari penyebaran berita hoaks, pembentukan opini palsu, hingga menjadi sebuah ancaman terhadap periode sensitif suatu negara seperti pada saat pemilihan umum dimana hal ini dapat memberikan rasa keraguan masyarakat terhadap sebuah institusi formal. Disinformasi visual berupa *deepfake* yang sudah terjadi pada abad ke 19 ini menjadi penanda bahwa penggunaan teknologi visual telah digunakan sebagai alat propaganda dalam cakupan global yang bekerja dengan cara menciptakan sebuah visual dan audio dari tokoh-tokoh politik dunia.

Rasa ketidakpercayaan terhadap teknologi dapat melemahkan hubungan publik dengan institusi negara nya dan mengarahkan ancaman perang antarnegara ke ranah digital. Dalam kasus Indonesia, undang-undang yang menjadi landasan hukum dari penyalahgunaan teknologi masih terbilang luas dan tidak bersifat eksklusif terhadap *deepfake*. Hal ini menjadi peringatan bagi Indonesia untuk membentuk sebuah proses hukum yang bersifat inklusif dan membentuk institusi yang berfokus pada digital *learning* untuk menjadi pondasi publik dalam menelaah informasi secara kritis. Potensi *deepfake* semakin meningkat dalam melakukan polarisasi sosial dan melemahkan kepercayaan publik terhadap institusi politik negara. Tanpa pengelolaan yang berkelanjutan *deepfake* dapat memberikan efek domino dalam perluasan disinformasi.

REFERENCES

Anri Syaiful, A. (2024). *INFOGRAFIS PASCA-SERANGAN RANSOMWARE KE PDN, KEMENTRIAN DAN LEMBAGA NEGARA WAJIB CADANGKAN DATA*. Diambil kembali dari Liputan 6: https://www.liputan6.com/news/read/5633579/infografis-pasca-serangan-ransomeware-ke-pdn-kementrian-dan-lembaga-negara-wajib-cadangkan-data?

APJII. (2024). *APJII JUMLAH PENGGUNA INTERNET INDONESIA TEMBUS 221 JUTA ORANG.* Asosiasi Penyelenggara Jasa Internet Indonesia. Diambil kembali dari Asosiasi Penyelenggara Jasa Internet Indonesia: https://apjii.or.id/berita/d/apjii-jumlah-penggua-internet-indonesia-tembus-221-juta-orang

Arvi Palindra, M. S. (2024). ANCAMAN DEEPFAKE BUATAN AI DAN IMPLIKASINYA TERHADAP KEAMANAN DATA BIOMETRIK DI INDONESIA. *Jurnal Spektrum Hukum*, 110-120.

Berger, P., & Luckmann, T. (1966). *THE SOCIAL OF REALITY.* Great Britain: Penguin University Books.

Cameron Martel, G. P. (2020). RELIANCE ON EMOTION PROMOTES BELIEF IN FAKE NEWS. *Cognitive Research: Principles and Implications*, 1-20.

Citron, B. C. (2019). DEEP FAKES: A LOOMING CHALLENGE FOR PRIVACY, DEMOCRACY, AND NATIONAL SECURITY. *Boston University School of Law*, 1762-1763.

Dhahir, D. F., & et al. (2024). THE RELATIONSHIP OF DIGITAL LITERACY, EXPOSURE TO AI-GENERATED DEEPFAKE VIDEOS, AND THE ABILITY TO IDENTIFY DEEPFAKES IN GENERATION X. *Jurnal Pekommas*, 358-365.

França, J. (2022). *WOLF, WOLF! ALARM OVER DISINFORMATION AND THE LIAR'S DIVIDEND*. Diambil kembali dari CCCBLAB: https://lab.cccb.org/en/wolf-wolf-alarm-over-disinformation-and-the-liars-dividend/

Gstalter, M. (2018). *'OBAMA' VOICED BY JORDAN PEELE IN PSA VIDEO WARNING ABOUT FAKE VIDEOS*. Diambil kembali dari THE HILL: https://thehill.com/blogs/in-the-know/in-the-know/383525-obama-voiced-by-jordan-peele-in-psa-video-warning-about-fake/

Hancock, J. T., & Bailenson, J. N. (2021). THE SOCIAL IMPACT OF DEEPFAKES. *CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING*, 149-152.

Harris, K. R. (2022). REAL FAKES: THE EPISTEMOLOGY OF ONLINE MISINFORMATION. *Philosophy & Technology*, 1-24.

Ian J. Goodfellow, J. P.-A., Mehdi Mirza, B. X.-F., & Sherjil Ozair, A. C. (2014). GENERATIVE ADVERSARIAL NETS. *arXiv*, 1-7.

INDOPOSCO.Id. (2024). *AWAS RUGI BANDAR TIDAK MEMANFAATKAN RUANG DIGITAL!* INDOPOSCO.Id.

Judijanto, L., & et al. (2025). IMPLEMENTATION OF ETHICAL ARTIFICIAL INTELLIGENCE LAW TO PREVENT THE USE OF AI IN SPREADING FALSE INFORMATION (DEEPFAKE) IN INDONESIA. *The Easta Journal Law and Human Rights*, 101-109.

Kaylyn Jackson Schiff, D. S., & Natalia Bueno. (2025). THE LIAR'S DIVIDEND: CAN POLITICIANS CLAIM MISINFORMATION TO EVADE ACCOUNTABILITY? *American Political Science Review*, 71-88.

KOMDIGI. (2023, Oktober 27). *[DISINFORMASI] VIDEO "PIDATO PRESIDEN JOKOWI DIDUGA MENGGUNAKAN BAHASA MANDARIN"*. Diambil kembali dari KOMDIGI Klarifikasi Hoaks: https://www.komdigi.go.id/berita/berita-hoaks/detail/disinformasi-video-pidato-presiden-jokowi-diduga-menggunakan-bahasa-mandarin

Komisi Pemilihan Umum Kota Salatiga. (2025, Maret 5https://kota-salatiga.kpu.go.id/blog/read/partisipasi-masyarakat-menurun-dalam-pemilihan-serentak-tahun-2024). *Partisipasi Masyarakat Menurun Dalam Pemilihan Seretetak Tahun 2024*. Diambil kembali dari KOMISI PEMILIHAN UMUM KOTA SALATIGA.

Kristiyenda, & et al. (2025). PENCEGAHAN KEJAHATAN DEEPFAKE; STUDI KASUS TERHADAP MODIS PENIPUAN DEEPFAKE PRABOWO SUBIANTO DALAM TAWARAN BANTUAN UANG. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 149-164.

Latifa, N. R. (2024). *APA ITU DEEPFAKE? TEKNOLOGI CANGGIH DENGAN POTENSI BERBAHAYA*. Diambil kembali dari Cyber Threats: https://sibermate.com/hrmi/apa-itu-deepfake-teknologi-canggih-dengan-potensi-berbahaya

Mirsky, Y., & Lee, W. (2020). THE CREATION AND DETECTION OF DEEPFAKES: A SURVEY. *arXiv*, 1-33.

Nestia Lianingsih, A. J. (2025). LEGAL IMPLICATIONS OF THE USE OF DEEPFAKE IN POLITICS AND NATIONAL SECURITY IN INDONESIA. *International Journal of Humanities, Law & Politics*, 6-14.

Paul, C., & Matthews, M. (2016). THE RUSSIAN "FIREHOUSE OF FALSEHOOD" PROPAGANDA MODEL. *RAND Corporation*, 1-15.

Pawelec, M. (2022). DEEPFAKES AND DEMOCRACY (THEORY): HOW SYNTHETIC AUDIO-VISUAL MEDIA FOR DISINFORMATION AND HATE SPEECH THREATEN CORE DEMOCRATIC FUNCTIONS. *Digital Society*, 1-37.

Presiden Republik Indonesia. (2022). *UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI (UU PDP) NO. 27 TAHUN 2022* . Peraturan Badan Pemeriksa Keuangan.

Republik Indonesia. (2016). *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016.* KEMENTRIAN PERTAHANAN REPUBLIK INDONESIA. Diambil kembali dari lembaran negara republik indonesia: https://www.kemhan.go.id/itjen/wp-content/uploads/2017/08/uu19-2016bt.pdf

Riyanto, D. (2024, Februari 21). *HOOTSUITE (WE ARE SOCIAL): DATA DIGITAL INDONESIA 2024*. Dipetik April 28, 2025, dari andi.link: https://andi.link /hootsuite-we-are-social-data-digital-indonesia-2024/

Rosy Saptoyo, K. E. (2024). *SURVEI APJII, HOAKS POLITIK MENDOMINASI MEDIA SOSIAL.* Kompas.com.

Szélpál, L. (2023). THE MAJOR INFLUENCE OF THOMAS NAST'S POLITICAL CARTOONS ON 19TH CENTURY AMERICAN POLITICS. *AMERICANA E-Journal of American Studies in Hungary*, 1-19.

T20 INDONESIA. (2022). *DEEPFAKES AND SECURITY IN THE INFORMATION ENVIROMENT: CHALLENGES FOR GOVERNMENTS, SOCIETY, AND BUSINESS.* T20 INDONESIA 2022.

Tulga, A. Y. (2024). BRIDGING DISCIPLINARY GAPS AND METHODOLOGICAL CHALLENGES IN UNDERSTANDING DEEPFAKE DISCOURSE: A STUDY OF TURKISH REDDIT POSTS RELATED TO DEEPFAKE. *Scaffold Press*, 51-59.

Vaccari, C., & Chadwick, A. (2020). DEEPFAKES AND DISINFORMATION: EXPLORING THE IMPACT OF SYNTHETIC POLITICAL VIDEO ON

DECEPTION, UNCERTAINTY, AND TRUST IN NEWS. *Social Meida + Society*, 1-10

We Are Social. (2024). *DIGITAL 2024: INDONESIA.* We Are Social USA.

Zahro, A. F. (2024). DAMPAK PENYALAHGUNAAN DEEPFAKE DALAM MEMANIPULASI VISUAL: MENGUAK POTENSI INFOCALYPSE DI ERA POST TRUTH TERHADAP ASUMSI MASYARAKAT PADA MEDIA MASSA. *Jurnal Kawistara: The Journal of Social Sciences and Humanities*, 402-412.