

**DISINFORMASI BERBASIS *ARTIFICIAL INTELLIGENCE* DAN KRISIS
KEPERCAYAAN PUBLIK DALAM *INFORMATION WARFARE* PADA
KONFLIK IRAN–AS–ISRAEL 2026: PERSPEKTIF HUKUM SIBER DAN
HUKUM PIDANA INTERNASIONAL**
***ARTIFICIAL INTELLIGENCE-BASED DISINFORMATION AND PUBLIC
TRUST CRISIS IN INFORMATION WARFARE DURING THE
ESCALATION OF THE 2026 IRAN–U.S.–ISRAEL CONFLICT: A
PERSPECTIVE OF CYBER LAW AND INTERNATIONAL CRIMINAL LAW***

Tomi Agi Fratama dan Priskila Kurniawati

Universitas Nusa Cendana

Korespondensi Penulis: tomi.fratama@staf.undana.ac.id,
priskila.kurniawati@staf.undana.ac.id

Citation Structure Recommendation :

Fratama, Tomi Agi dan Priskila Kurniawati. *Disinformasi Berbasis Artificial Intelligence dan Krisis Kepercayaan Publik dalam Information Warfare pada Konflik Iran–As–Israel 2026: Perspektif Hukum Siber dan Hukum Pidana Internasional*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.1 (2026).

ABSTRAK

Perkembangan *Artificial Intelligence* (AI) telah meningkatkan kemampuan produksi dan penyebaran disinformasi dalam konflik internasional. Eskalasi konflik Iran–AS–Israel tahun 2026 memperlihatkan penggunaan konten sintesis, deepfake dan manipulasi informasi digital sebagai bagian dari information warfare. Penelitian ini bertujuan menganalisis kedudukan hukum disinformasi berbasis AI dalam perspektif hukum siber dan hukum pidana internasional. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual dan kasus. Hasil penelitian menunjukkan bahwa disinformasi berbasis AI belum diatur sebagai tindak pidana tersendiri dalam hukum internasional. Dalam perspektif hukum siber, penggunaan AI untuk menyebarkan disinformasi dapat berkaitan dengan cybercrime apabila memenuhi unsur tindak pidana siber tertentu. Sementara itu, hukum pidana internasional membuka kemungkinan pertanggungjawaban apabila disinformasi digunakan untuk mendukung atau memfasilitasi pelaksanaan kejahatan internasional yang menjadi yurisdiksi Statuta Roma.

Kata Kunci: *Artificial Intelligence*, Disinformasi, Hukum Pidana Internasional, Hukum Siber, Information Warfare

ABSTRACT

The development of Artificial Intelligence (AI) has significantly enhanced the creation and dissemination of disinformation in international conflicts. The escalation of the 2026 Iran–U.S.–Israel conflict demonstrated the use of synthetic content, deepfakes and digital information manipulation as instruments of information warfare. This study aims to analyze the legal status of AI-based disinformation from the perspectives of cyber law and international criminal law. The research employs a normative legal method using statutory, conceptual and case approaches. The findings indicate that AI-based disinformation has not yet been recognized as a distinct criminal offense under international law. From a cyber law perspective, the use of AI to disseminate disinformation may be associated with cybercrime if it fulfills the elements of specific cyber offenses. Furthermore, international criminal law provides the possibility of liability when disinformation is used to support or facilitate the commission of international crimes within the jurisdiction of the Rome Statute.

Keywords: *Artificial Intelligence, Cyber Law, Disinformation, Information Warfare, International Criminal Law*

A. PENDAHULUAN

Perkembangan *Artificial Intelligence* (AI) telah mengubah lanskap produksi dan distribusi informasi dalam ruang digital. Teknologi generatif memungkinkan pembuatan teks, gambar, audio dan video sintetis dengan tingkat kemiripan yang tinggi sehingga semakin sulit dibedakan dari konten autentik. Kondisi tersebut melahirkan tantangan baru berupa penyebaran hoaks, disinformasi dan manipulasi informasi yang dilakukan secara lebih cepat, masif dan terstruktur. Salah satu bentuk paling banyak mendapat perhatian ialah penggunaan deepfake dan konten sintetis berbasis AI yang mampu membentuk persepsi publik, memengaruhi opini politik, serta menurunkan kepercayaan masyarakat terhadap informasi resmi.¹

Kemajuan dari teknologi kecerdasan buatan tersebut 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 (GANs) yang mana mampu menciptakan citra dan suara tokoh publik secara sintesis dengan ketepatan yang mengkhawatirkan.²

¹ 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, Vol.4, No.1 (2025), p.73-92.

² Nur Rachmi Latifa, *Apa Itu Deepfake? Teknologi Canggih dengan Potensi Berbahaya*, "Cyber Threats", diakses dari <https://sibermate.com/hrmi/apa-itu-deepfake-teknologi-canggih-dengan-potensi-berbahaya>, diakses pada 22 Juni 2026.

Kemudahan akses terhadap perangkat lunak open-source menjadikan pembuatan video palsu kini bukan lagi domain eksklusif 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.

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*.³ 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. Disinformasi berbasis AI tidak selalu dapat dikategorikan sebagai cybercrime, suatu tindakan baru dapat dikategorikan sebagai tindak pidana siber apabila memenuhi unsur-unsur delik tertentu yang diatur dalam hukum nasional maupun instrumen internasional tentang kejahatan siber. Persoalan menjadi semakin kompleks ketika penyebaran informasi dilakukan melalui platform digital lintas negara, melibatkan jaringan otomatis, akun anonim, atau infrastruktur teknologi yang berada di berbagai yurisdiksi. Karakter transnasional ini dapat menimbulkan tantangan dalam penegakan hukum, pembuktian elektronik, atribusi pelaku dan penentuan yurisdiksi negara yang berwenang. 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.⁴

Persoalan lain yang muncul dalam perspektif hukum pidana internasional. Hingga saat ini belum ada instrumen internasional khusus yang mengatur disinformasi berbasis AI sebagai suatu kejahatan internasional yang mandiri.

³ Ahmet Yiğitalp Tulga, *Bridging Disciplinary Gaps and Methodological Challenges in Understanding Deepfake Discourse: A Study of Turkish Reddit Posts Related to Deepfake*, Scaffold: Journal of the Institute of Comparative Studies in Literature, Arts and Culture, Vol.1, No.2 (2024), p.51-59.

⁴ M. Gstalter, *Obama' Voiced by Jordan Peele in PSA Video Warning about Fake Videos*, diakses dari <https://thehill.com/blogs/in-the-know/in-the-know/383525-obama-voiced-by-jordan-peele-in-psa-video-warning-about-fake/>, diakses pada 22 Juni 2026.

Statuta Roma Mahkamah Pidana Internasional belum mengakui disinformasi digital sebagai salah satu kategori tindak pidana internasional. Meskipun demikian, penggunaan informasi palsu secara sistematis dalam situasi konflik bersenjata tetap memiliki relevansi hukum apabila terbukti digunakan untuk membantu, memfasilitasi, atau mendukung pelaksanaan kejahatan internasional yang menjadi yurisdiksi Mahkamah Pidana Internasional. Oleh karena itu, hubungan antara disinformasi digital, information warfare dan pertanggungjawaban pidana internasional masih menjadi topik perdebatan yang berkembang dalam literatur hukum kontemporer.⁵

Perkembangan teknologi *Artificial Intelligence* menyebabkan manipulasi wajah, suara, maupun video dapat dilakukan dengan tingkat kemiripan yang sangat tinggi sehingga sulit dibedakan dari konten asli. Kondisi tersebut menimbulkan ancaman serius terhadap perlindungan hak privasi, reputasi dan keamanan digital masyarakat.⁶

Salah satu karakteristik utama deepfake terletak pada kemampuannya memalsukan ekspresi wajah, gerakan tubuh dan suara seseorang secara realistis. Rekaman visual dan audio digunakan sebagai data pelatihan sehingga algoritma mampu menghasilkan konten digital yang sulit dibedakan dari video asli. Kondisi tersebut menjadikan deepfake sebagai ancaman serius dalam bidang hukum, politik dan media sosial.⁷ Perkembangan teknologi Generative Adversarial Networks (GANs) turut memperkuat kemampuan manipulasi digital. Sistem GANs bekerja melalui dua komponen utama, yaitu generator yang menciptakan konten palsu dan discriminator yang membandingkan hasil manipulasi dengan data asli. Proses pembelajaran yang berlangsung secara terus-menerus menyebabkan hasil manipulasi menjadi semakin sulit dideteksi, bahkan oleh ahli forensik digital.⁸

⁵ Silvia Maharani Iskandar Putri, Nashwa Salsabila dan Asmak U. I. Hosnah, *Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum*, Jurnal Hukum Legalita, Vol.6, No.2 (2024), p.83-90.

⁶ Natanael Hiskia Mongkau, Herlyanty Yuliana A. Bawole dan Altje Musa, *Penegakkan Hukum terhadap Penyalahgunaan Kecerdasan Buatan dengan Cara Memanipulasi Wajah Seseorang ke dalam Gambar atau Video Porno*, Lex Administratum, Vol.13, No.2 (2025).

⁷ Bramcov Stivens Situmeang, dkk., *Pengaruh Artificial Intelligence terhadap Tingkat Kasus Deep Fake pada Selebritas di Twitter*, Device, Vol.14, No.1 (2024), p.80-91.

⁸ Bonda Sisephaputra, dkk., *Generative Artificial Intelligence (GenAI): Pengetahuan Dasar GenAI Beserta Penerapannya*, Green Pustaka Indonesia, Yogyakarta, 2024.

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. 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.

Indonesia hingga saat ini belum memiliki regulasi khusus yang secara eksplisit mengatur *deepfake* sebagai tindak pidana tersendiri. Beberapa ketentuan dalam peraturan perundang-undangan tetap dapat digunakan untuk menjerat pelaku penyebaran konten *deepfake*. Perkembangan teknologi yang bergerak sangat cepat menimbulkan tantangan besar dalam penegakan hukum, terutama dalam aspek pembuktian dan pertanggungjawaban pidana.⁹

Ketentuan hukum mengenai penyebaran informasi palsu dalam ruang digital saat ini mengacu pada Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ketentuan yang relevan terdapat dalam Pasal 28 ayat (1) yang menyatakan:¹⁰

“Setiap Orang dengan sengaja dan tanpa hak menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang dapat menimbulkan kerusakan di masyarakat.”

Ketentuan dari undang-undang ini menunjukkan bahwa hukum positif Indonesia telah menetapkan batasan terhadap penyebaran informasi elektronik yang tidak benar dan berpotensi menimbulkan gangguan ketertiban umum.

⁹ Yolanda Frisky Amelia, Arfan Kaimuddin dan Hisbul Luthfi Ashsyarofi, *Pertanggungjawaban Pidana Pelaku terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake menurut Hukum Positif Indonesia*, Dinamika: Jurnal Ilmiah Ilmu Hukum, Vol.30, No.1 (2024), p.9675-9691.

¹⁰ Indonesia, *Undang-Undang tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Pasal 28 ayat (1) UU No.1 Tahun 2024, LN Tahun 2024 No.1, TLN No.6905.

Relevansi pasal ini terlihat dari penggunaan *Artificial Intelligence* untuk menghasilkan maupun menyebarkan konten disinformasi yang dirancang untuk memengaruhi persepsi publik melalui informasi yang tidak sesuai dengan fakta.

Dampak penyebaran disinformasi tidak selalu berhenti pada penyampaian informasi bohong semata. Dalam praktiknya, konten yang dihasilkan melalui teknologi *Artificial Intelligence* juga dapat digunakan untuk membangun narasi yang menimbulkan kebencian, permusuhan, maupun polarisasi sosial terhadap individu atau kelompok tertentu. Penggunaan deepfake, manipulasi audio-visual, maupun narasi palsu berpotensi memperkuat sentimen identitas dan mendorong terbentuknya pandangan negatif terhadap kelompok tertentu secara masif melalui media elektronik. Risiko tersebut mendapat perhatian dalam Pasal 28 ayat (2) Undang-Undang Nomor 1 Tahun 2024 yang menyatakan:¹¹

“Setiap Orang dengan sengaja dan tanpa hak menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi hasutan kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat berdasarkan suku, agama, ras dan antargolongan (SARA).”

Ketentuan ini menunjukkan bahwa perlindungan hukum tidak hanya berlaku terhadap penyebaran berita palsu, tetapi juga terhadap penggunaan media elektronik yang dapat memicu kebencian dan permusuhan berdasarkan identitas. Dalam konteks konflik Iran–AS–Israel 2026, penyebaran disinformasi berbasis *Artificial Intelligence* berpotensi digunakan untuk memperkuat sentimen keagamaan, kebangsaan, maupun identitas kelompok tertentu sehingga mempengaruhi opini publik dan memperdalam polarisasi sosial di ruang digital.

Persoalan lain muncul dalam aspek pembuktian hukum. Konten deepfake sering kali sulit dibedakan dari video asli sehingga membutuhkan teknologi forensik digital yang memadai untuk mendeteksinya. Indonesia masih menghadapi keterbatasan dalam pengembangan teknologi pendeteksi deepfake, sehingga proses investigasi terhadap kasus manipulasi digital menjadi lebih kompleks. Kerja sama antara penegak hukum, akademisi dan pakar teknologi diperlukan untuk membangun metode identifikasi dan analisis konten deepfake guna mendukung proses penegakan hukum. Tantangan berikutnya berkaitan dengan peran platform media sosial dalam menangani penyebaran deepfake.

¹¹ *Ibid.*.

Platform seperti Facebook, TikTok dan YouTube telah mengembangkan kebijakan untuk mendeteksi dan menghapus konten manipulatif yang bersifat menyesatkan atau berbahaya. Efektivitas kebijakan tersebut masih terbatas karena banyak konten deepfake tetap beredar luas sebelum akhirnya dihapus. Kondisi tersebut mendorong perlunya penguatan regulasi yang mewajibkan platform digital bertindak lebih proaktif dalam menangani penyebaran deepfake, sebagaimana diterapkan Uni Eropa melalui *Digital Services Act* (DSA).¹²

Fenomena ini semakin terlihat melalui peningkatan konflik antara Iran, Amerika Serikat dan Israel pada tahun 2026. Selain memperlihatkan konfrontasi militer, konflik ini juga ditandai oleh maraknya penyebaran konten digital yang menampilkan rekaman serangan, pernyataan pejabat, maupun dokumentasi korban yang kemudian dipersoalkan keasliannya. Berbagai laporan pemeriksa fakta menunjukkan beredarnya gambar, video dan narasi yang dihasilkan atau dimanipulasi menggunakan teknologi AI yang dapat memengaruhi persepsi publik internasional mengenai jalannya konflik. Situasi ini menunjukkan bahwa ruang digital telah berkembang menjadi arena information warfare yang digunakan untuk membangun legitimasi politik, memengaruhi opini di tingkat global, serta mendapatkan keuntungan strategis dalam berbagai konflik internasional.

Di era *post-truth*, publik semakin dihadapkan pada sebuah pilihan apakah ingin mencari tahu kebenaran suatu informasi yang didapatkan ataupun langsung percaya dengan informasi itu sehingga berpengaruh langsung terhadap keyakinan pribadi dan emosi pribadi. Urgensi penelitian ini semakin jelas terlihat terutama karena dengan tingginya penggunaan internet dan media digital. Survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) Tahun 2025 menunjukkan bahwa tingkat penetrasi internet Indonesia mencapai 80,66 persen atau sekitar 229,43 juta pengguna.¹³ Meningkatnya penggunaan media digital memperbesar risiko penyebaran informasi palsu dan manipulatif yang dapat memengaruhi persepsi publik secara luas. Kondisi ini memperlihatkan bahwa persoalan disinformasi berbasis AI tidak hanya menjadi isu teknologi,

¹² Hendra Prayoga Hadi Tuasikal, *Penyebaran Konten Deepfake sebagai Tindak Pidana: Analisis Kritis terhadap Penegakan Hukum dan Perlindungan Publik di Indonesia*, Abdurrauf Law and Sharia, Vol.2, No.1 (2025), p.22-38.

¹³ Asosiasi Penyelenggara Jasa Internet Indonesia, *Survei Penetrasi Internet Indonesia 2025*, Asosiasi Penyelenggara Jasa Internet Indonesia, Jakarta, 2025.

tetapi juga berkaitan dengan aspek hukum, keamanan dan ketertiban di tingkat internasional.¹⁴

Dalam perspektif hukum, fenomena tersebut dapat dikaji dalam dua dimensi: pertama, sebagai bagian dari *information warfare*; kedua, sebagai potensi tindak pidana siber lintas negara (*transnational cybercrime*) integrasi teknologi digital dalam produksi informasi telah menciptakan tantangan serius terhadap tata kelola hukum dan legitimasi publik. Ketika informasi yang dimanipulasi disebarkan secara masif dan terstruktur untuk memengaruhi persepsi global, tindakan tersebut tidak lagi sekadar persoalan etika komunikasi, melainkan dapat masuk dalam kategori penyalahgunaan sistem elektronik yang berdampak luas.¹⁵

Perkembangan AI generatif memperbesar potensi tersebut AI memungkinkan produksi hoaks dalam bentuk teks, gambar dan video yang sangat realistis, sehingga sulit dibedakan dari konten asli.¹⁶ Dalam situasi konflik bersenjata, penggunaan teknologi deepfake atau manipulasi audiovisual dapat digunakan untuk memicu kepanikan publik, menyebarkan propaganda, atau bahkan memprovokasi eskalasi militer. sebagai bentuk baru kejahatan berbasis deepfake yang berpotensi merugikan kepentingan publik dan keamanan nasional.¹⁷

Tantangan yang dihadapi bukan hanya bersifat teknis tetapi juga budaya dan pendidikan. Literasi media sosial sangat penting untuk mengurangi dampak negatif penyebaran berita palsu menggunakan teknologi AI. Literasi media bukan hanya tentang membaca informasi; tetapi juga mencakup kemampuan untuk mengidentifikasi sumber, memahami cara kerja algoritma, mengenali teknik manipulasi digital dan mengevaluasi konten yang diterima tersebut secara kritis.

¹⁴ N. Amaly dan Armiah, *Media Digital dan Tantangan Disinformasi di Era Society 5.0*, Jurnal Ilmu Komunikasi, Vol.9, No.1 (2021), p.50.

¹⁵ Dimas Tri Wicaksono, Friyandi Prasetya dan Niken Putri Lestari, *Penegakan Hukum Terhadap Kejahatan Deepfake dalam Perspektif Hukum Positif Indonesia*, Jurnal Fakta Hukum, Vol.4, No.2 (Maret 2026).

¹⁶ Christiany Juditha, *Artificial Intelligence dan Tantangan Disinformasi Digital di Media Sosial*, Jurnal Penelitian Komunikasi dan Opini Publik, Vol.29, No.1 (2025), p.41.

¹⁷ Ahmad Ihsan dan Evy Nurmiati, *Akuntabilitas Profesional di Era Deepfake: Analisis Etika dan Strategi Mitigasi Penipuan Digital dalam Sistem Informasi*, Kohesi: Jurnal Multidisiplin Saintek, Vol.10, No.11 (2026).

Beberapa studi menunjukkan bahwa orang dengan literasi digital yang baik umumnya lebih mampu mengenali berita palsu dan mengendalikan diri untuk tidak menyebarkannya lebih lanjut. Hal ini menunjukkan bahwa literasi media merupakan strategi kunci dalam mengatasi masalah disinformasi digital, termasuk ketika berita palsu diproduksi dan disebar dengan bantuan teknologi canggih.¹⁸

Dalam konteks hukum siber internasional, penyebaran konten manipulatif yang disengaja dan terkoordinasi dapat dikategorikan sebagai bagian dari *cyber-enabled* disinformation operations. Praktik tersebut berpotensi melanggar norma internasional terkait intervensi terhadap kedaulatan negara lain, terutama apabila dilakukan oleh aktor negara atau didukung secara sistematis oleh entitas tertentu. Dalam beberapa diskursus hukum internasional, operasi informasi yang terkoordinasi bahkan diperdebatkan dalam konteks hybrid warfare, yakni kombinasi antara serangan militer, serangan siber dan manipulasi informasi.

Manipulasi digital yang digunakan untuk menyebarkan kebencian, memicu kekerasan terhadap kelompok tertentu, atau memalsukan bukti terkait pelanggaran hukum humaniter berpotensi bersinggungan dengan rezim hukum pidana internasional. Pengaturan dalam Statuta Roma Mahkamah Pidana Internasional belum secara eksplisit memasukkan disinformasi digital sebagai bentuk kejahatan tersendiri. Penggunaan informasi palsu yang mendukung terjadinya kejahatan perang atau kejahatan terhadap kemanusiaan tetap memiliki implikasi hukum, terutama dalam proses pembuktian serta penentuan pertanggungjawaban pidana.

Dimensi cybercrime terlihat melalui pelanggaran terhadap sistem elektronik, penyebaran konten palsu yang merugikan publik, serta keterlibatan jaringan bot atau otomatisasi digital lintas negara. Karakter lintas batas dari media sosial memperumit proses penegakan hukum. Konten dapat diproduksi di satu negara, disebar melalui server di negara lain, lalu menimbulkan dampak di wilayah yang berbeda. Kondisi ini memunculkan persoalan mengenai kompetensi yurisdiksi, kebutuhan kerja sama internasional, serta tanggung jawab platform digital dalam mengelola dan mengendalikan distribusi informasi.

¹⁸ Dudi Iskandar, Geri Suratno dan Didik Hariyadi Raharjo, *Construction of Digital Literacy in the 2024 Election to Stem the Flow of Hoax and Fake News*, Ekspresi dan Persepsi: Jurnal Ilmu Komunikasi, Vol.7, No.2 (Mei 2024).

Akumulasi praktik ini berdampak pada krisis kepercayaan publik. Ketika masyarakat global tidak lagi mampu membedakan antara dokumentasi faktual dan manipulasi digital, legitimasi informasi resmi menjadi tergerus. Dalam konteks konflik bersenjata, krisis kepercayaan ini dapat memengaruhi persepsi terhadap pelanggaran hukum humaniter internasional, klaim korban sipil dan proses diplomatik. Dengan demikian, disinformasi berbasis AI bukan hanya persoalan komunikasi, tetapi juga persoalan hukum dan keamanan internasional.

Berbagai penelitian telah membahas deepfake, disinformasi digital dan literasi media dalam perspektif keamanan siber maupun komunikasi digital. Fokus kajian yang berkembang masih didominasi oleh aspek teknis deteksi konten manipulatif dan dampak sosial penyebaran informasi palsu. Pembahasan mengenai pemanfaatan *Artificial Intelligence* sebagai instrumen information warfare dalam konflik bersenjata internasional masih terbatas, khususnya yang menjadikan konflik Iran–AS–Israel tahun 2026 sebagai objek kajian. Di samping itu, belum banyak penelitian yang mengkaji keterkaitan antara penyebaran disinformasi berbasis AI dengan konsep cybercrime serta kemungkinan pertanggungjawaban dalam hukum pidana internasional. Kekosongan kajian tersebut menjadi dasar penting bagi penelitian ini untuk menganalisis disinformasi berbasis *Artificial Intelligence* dalam konflik Iran–AS–Israel 2026 melalui perspektif hukum siber dan hukum pidana internasional.¹⁹

Berdasarkan penjelasan tersebut, penelitian ini mengajukan dua rumusan masalah. Pertama, bagaimana penyebaran disinformasi berbasis *Artificial Intelligence* dalam konflik Iran–AS–Israel 2026 dapat dikualifikasikan dalam perspektif hukum siber? Kedua, bagaimana pertanggungjawaban dalam hukum pidana internasional terhadap penggunaan disinformasi berbasis *Artificial Intelligence* dalam information warfare pada konflik Iran–AS–Israel 2026?.

B. PEMBAHASAN

1. Penyebaran Disinformasi Berbasis *Artificial Intelligence* dalam konflik Iran–AS–Israel 2026 dapat Dikualifikasikan sebagai Cybercrime dalam Perspektif Hukum Siber

¹⁹ *Ibid.*.

a. Disinformasi sebagai Persoalan *Platform Governance*

Penyebaran disinformasi berbasis *Artificial Intelligence* tidak selalu dapat dikualifikasikan sebagai tindak pidana siber. Sebagian besar konten manipulatif yang beredar dalam media sosial pada dasarnya berada dalam ranah tata kelola platform digital (*platform governance*). Platform seperti X, Facebook, TikTok dan YouTube memiliki kebijakan internal untuk menghapus, membatasi distribusi, atau memberikan label terhadap konten yang dinilai menyesatkan, termasuk konten hasil manipulasi *Artificial Intelligence*. Dalam konteks ini, penyebaran informasi palsu lebih banyak dipandang sebagai pelanggaran terhadap standar komunitas dan kebijakan pengelolaan konten dibandingkan sebagai tindak pidana.²⁰

Unsur perbuatan tercermin dari aktivitas produksi, manipulasi dan distribusi informasi melalui sistem elektronik. Konten berbasis AI seperti deepfake, rekayasa visual, serta narasi sintetis diproduksi secara sistematis dengan memanfaatkan teknologi komputasi dan disebarluaskan melalui platform digital lintas negara. Karakter ini menunjukkan adanya penggunaan sarana elektronik sebagai medium utama, yang dalam konteks hukum siber menjadi indikator penting dalam mengkualifikasikan suatu perbuatan sebagai cybercrime. Selain itu, sifat distribusi yang masif dan otomatis memperlihatkan adanya intensifikasi perbuatan yang melampaui pola konvensional penyebaran informasi.

Unsur kesalahan terletak pada adanya kesengajaan (*dolus*) dalam menciptakan dan menyebarkan informasi yang tidak benar. Disinformasi berbasis Kecerdasan Buatan (AI) tidak muncul secara spontan, melainkan melalui proses perancangan yang terstruktur dengan tujuan memengaruhi persepsi publik. Pelaku memiliki pengetahuan bahwa informasi yang diproduksi tidak sesuai dengan fakta serta memahami potensi akibat yang ditimbulkan. Pemahaman ini sejalan dengan konsep kesengajaan dalam hukum pidana yang mencakup unsur kehendak dan pengetahuan terhadap akibat yang mungkin terjadi.²¹ Dalam konteks ini,

²⁰ *Ibid.*

²¹ C. Wardle dan H. Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe, Strasbourg, 2017, p.20-27.

kesengajaan dapat berbentuk *dolus directus* maupun *dolus eventualis*, mengingat pelaku menyadari kemungkinan timbulnya dampak luas dari penyebaran informasi tersebut.

Unsur akibat terlihat dari dampak yang ditimbulkan dalam ruang sosial dan digital. Disinformasi berbasis AI tidak hanya menimbulkan kerugian individual, tetapi juga berdampak pada kepentingan hukum yang lebih luas, seperti terganggunya ketertiban umum, rusaknya kepercayaan publik, serta terdistorsinya informasi dalam konteks konflik internasional. Dalam situasi konflik Iran–AS–Israel, dampak tersebut dapat berkembang menjadi instrumen propaganda yang memengaruhi opini global serta legitimasi tindakan militer. Akibat ini memperlihatkan bahwa disinformasi memiliki dimensi kolektif yang melampaui kerugian individual semata.

b. Disinformasi sebagai Tindak Pidana Siber Menurut Hukum Nasional

Penggunaan *Artificial Intelligence* dalam produksi dan penyebaran disinformasi tidak serta-merta dapat dikualifikasikan sebagai tindak pidana siber. Kualifikasi tersebut bergantung pada terpenuhinya unsur-unsur delik yang diatur dalam peraturan perundang-undangan. Dalam hukum positif Indonesia, pengaturan mengenai penyebaran informasi elektronik yang mengandung unsur kebohongan maupun kebencian diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pengaturan terdapat dalam Pasal 28 ayat (2) yang menyatakan:

“Setiap Orang dengan sengaja dan tanpa hak menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi hasutan kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat berdasarkan suku, agama, ras dan antargolongan (SARA).”

Ketentuan ini memiliki relevansi yang lebih kuat dalam konteks konflik internasional karena disinformasi digital sering digunakan untuk memperkuat sentimen identitas, membangun propaganda kebencian dan memperdalam polarisasi sosial. Konten berbasis *Artificial Intelligence* dapat dimanfaatkan untuk menciptakan narasi yang menargetkan kelompok tertentu berdasarkan identitas agama, etnis, maupun afiliasi politik. Dalam situasi konflik Iran–AS–Israel, penyebaran konten manipulatif yang memanfaatkan isu identitas berpotensi memperluas permusuhan, memperkuat stereotip dan memengaruhi persepsi masyarakat internasional terhadap pihak-pihak yang terlibat dalam konflik.

Pengaturan tersebut menunjukkan bahwa disinformasi berbasis *Artificial Intelligence* tidak secara otomatis dapat dikategorikan sebagai *cybercrime*. Kualifikasi sebagai tindak pidana siber baru dapat dilakukan apabila penyebaran informasi memenuhi unsur-unsur delik yang telah ditentukan dalam peraturan perundang-undangan, termasuk adanya unsur kesengajaan (*mens rea*), perbuatan menyebarkan informasi elektronik, serta akibat hukum yang ditimbulkan. Oleh karena itu, pendekatan hukum terhadap disinformasi berbasis *Artificial Intelligence* harus dilakukan secara hati-hati dengan mempertimbangkan karakteristik perbuatan dan unsur tindak pidana yang relevan.

Ketentuan tersebut diperkuat oleh Pasal 45A ayat (2) Undang-Undang Nomor 1 Tahun 2024 yang menyatakan:

"Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi hasutan kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat berdasarkan suku, agama, ras dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."

Norma sanksi tersebut menunjukkan bahwa hukum positif Indonesia tidak hanya melarang penyebaran informasi elektronik yang mengandung unsur kebencian atau permusuhan berbasis SARA, tetapi juga memberikan konsekuensi pidana yang tegas terhadap pelakunya. Dalam konteks disinformasi berbasis *Artificial Intelligence*, ketentuan ini dapat memiliki relevansi apabila teknologi AI digunakan untuk menghasilkan atau menyebarkan konten manipulatif yang bertujuan membangkitkan kebencian, permusuhan, atau polarisasi sosial berdasarkan identitas tertentu. Namun demikian, penerapan pasal ini tetap harus didasarkan pada pembuktian unsur kesengajaan (*mens rea*), tujuan penyebaran, serta hubungan antara konten yang disebar dan dampak yang ditimbulkan di masyarakat.

c. Analisis Yurisdiksi, Atribusi, *Mens Rea*, *Causal Link* dan *Evidentiary Standard* dalam Disinformasi Berbasis *Artificial Intelligence*

Penyebaran disinformasi berbasis *Artificial Intelligence* dalam konflik Iran–AS–Israel 2026 tidak hanya menimbulkan persoalan mengenai pemenuhan unsur tindak pidana, tetapi juga menghadirkan tantangan dalam aspek yurisdiksi, atribusi pelaku, unsur kesalahan, hubungan kausal, serta pembuktian elektronik. Karakter ruang siber yang bersifat lintas batas menyebabkan suatu konten dapat diproduksi di satu negara, disimpan melalui server di negara lain dan menimbulkan dampak hukum di wilayah yang berbeda. Kondisi ini memunculkan persoalan mengenai negara mana yang memiliki kewenangan untuk melakukan penyelidikan, penuntutan dan penjatuhan sanksi terhadap pelaku penyebaran disinformasi digital.²²

Persoalan yurisdiksi semakin kompleks saat penyebaran informasi dilakukan melalui platform digital global yang beroperasi pada berbagai wilayah hukum. Dalam hukum siber internasional, pendekatan yurisdiksi tidak hanya didasarkan pada lokasi pelaku (*territorial jurisdiction*), tetapi juga dapat mempertimbangkan lokasi akibat yang ditimbulkan (*effects doctrine*) serta kepentingan negara yang terdampak oleh perbuatan itu.

²² Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Refika Aditama, Bandung, 2012, p.44-49.

Oleh karena itu, penentuan yurisdiksi terhadap disinformasi berbasis *Artificial Intelligence* memerlukan kerja sama lintas negara agar penegakan hukum tidak terhambat oleh batas-batas teritorial.²³

Selain yurisdiksi, persoalan penting lainnya adalah atribusi (*attribution*). Atribusi berkaitan dengan identifikasi pihak yang bertanggung jawab atas produksi dan penyebaran informasi manipulatif. Dalam hukum internasional, suatu tindakan baru dapat dikaitkan kepada negara apabila dilakukan oleh organ negara atau pihak lain yang bertindak atas instruksi, arahan, atau kendali negara. Permasalahan atribusi menjadi semakin rumit dalam operasi digital karena penyebaran informasi sering dilakukan melalui akun anonim, jaringan bot, sistem otomatis, maupun kelompok digital yang tidak mudah dihubungkan dengan individu atau negara tertentu.²⁴ Kesulitan atribusi semakin meningkat ketika teknologi *Artificial Intelligence* digunakan untuk menghasilkan konten secara otomatis sehingga hubungan antara pelaku dan hasil manipulasi menjadi lebih sulit dibuktikan. Akibatnya, penentuan tanggung jawab hukum memerlukan identifikasi yang jelas mengenai siapa yang mengendalikan, memerintahkan, atau memperoleh manfaat dari penyebaran informasi tersebut.²⁵

Aspek lain yang tidak kalah penting adalah unsur kesalahan (*mens rea*). Hukum pidana mensyaratkan adanya kesengajaan atau setidaknya pengetahuan mengenai akibat yang mungkin timbul dari suatu perbuatan. Dalam konteks disinformasi berbasis *Artificial Intelligence*, unsur kesengajaan dapat terlihat ketika pelaku mengetahui bahwa informasi yang diproduksi tidak sesuai dengan fakta, namun tetap menyebarkannya dengan tujuan memengaruhi opini publik, membangun propaganda, atau menciptakan persepsi tertentu terhadap suatu konflik. Pembuktian unsur ini menjadi penting karena tidak semua informasi yang ternyata keliru dapat secara otomatis dikategorikan sebagai tindak pidana.²⁶

²³ *Ibid.*.

²⁴ Pasal 4 dan Pasal 8 International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, 2001.

²⁵ Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues and Outcomes*, Northeastern University Press, Boston, 2012, p.102-111.

²⁶ Eddy O.S. Hiarij, *Prinsip-Prinsip Hukum Pidana*, Cahaya Atma Pustaka, Yogyakarta, 2016, p.156-163.

Penetapan pertanggungjawaban juga memerlukan adanya hubungan kausal (*causal link*) antara perbuatan dan akibat yang ditimbulkan. Hubungan kausal diperlukan untuk membuktikan bahwa penyebaran informasi manipulatif benar-benar berkontribusi terhadap kerugian, kepanikan publik, meningkatnya permusuhan, atau dampak lain yang menjadi dasar penjatuhan sanksi hukum. Dalam konflik internasional, pembuktian hubungan kausal menjadi lebih rumit karena opini publik sering dipengaruhi oleh berbagai faktor lain di luar informasi yang disebarakan melalui media digital.²⁷

Tantangan berikutnya berkaitan dengan standar pembuktian (*evidentiary standard*). Teknologi deepfake, manipulasi visual dan rekayasa audio menyebabkan proses autentikasi alat bukti elektronik menjadi semakin kompleks. Penegak hukum memerlukan dukungan forensik digital untuk membedakan antara konten autentik dan konten hasil manipulasi Artificial Intelligence. Verifikasi metadata, analisis sumber distribusi, pelacakan aktivitas akun digital, serta pemeriksaan terhadap sistem yang digunakan untuk menghasilkan konten menjadi bagian penting dalam proses pembuktian. Tanpa dukungan pembuktian elektronik yang memadai, proses penegakan hukum terhadap penyebaran disinformasi berbasis *Artificial Intelligence* akan menghadapi kesulitan dalam membuktikan keterlibatan pelaku maupun hubungan antara tindakan dan akibat yang ditimbulkan.²⁸

Analisis mengenai yurisdiksi, atribusi, *mens rea*, *causal link* dan *evidentiary standard* menunjukkan bahwa penanganan disinformasi berbasis *Artificial Intelligence* tidak cukup hanya dengan mengidentifikasi keberadaan informasi palsu. Penegakan hukum juga harus mampu membuktikan keterkaitan antara pelaku, perbuatan dan akibat yang timbul melalui mekanisme pembuktian yang dapat dipertanggungjawabkan secara hukum.²⁹

²⁷ *Ibid.*.

²⁸ Josua Sitompul, *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Tatanusa, Jakarta, 2012, p.95-101; Council of Europe, *Convention on Cybercrime* (Budapest Convention), 2001.

²⁹ Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*, Kencana, Jakarta, 2013, p.78-84.

2. Bagaimana Pertanggungjawaban dalam Hukum Pidana Internasional terhadap Penggunaan Disinformasi Berbasis *Artificial Intelligence* dalam Information Warfare pada konflik Iran–AS–Israel 2026

Pertanggungjawaban dalam hukum pidana internasional terhadap penggunaan disinformasi digital berbasis *Artificial Intelligence* berkaitan dengan hubungan antara tindakan, akibat, serta keterkaitan perbuatan tersebut dengan kategori kejahatan internasional. Perubahan pola konflik modern telah memperluas arena peperangan dari penggunaan kekuatan militer menuju perebutan pengaruh dalam ruang digital. Informasi dipergunakan untuk membentuk persepsi publik, memengaruhi legitimasi politik, serta mengarahkan opini internasional terhadap suatu konflik bersenjata. Meskipun demikian, keberadaan informasi palsu dalam ruang digital tidak serta-merta dapat dikualifikasikan sebagai tindak pidana maupun kejahatan internasional. Penentuan tanggung jawab hukum harus dilakukan berdasarkan kategori dan karakteristik perbuatan yang dilakukan.³⁰

a. Disinformasi sebagai Pelanggaran Administratif dan *Platform Governance*

Konflik Iran–AS–Israel memperlihatkan penggunaan *Artificial Intelligence* dalam produksi propaganda digital melalui deepfake, manipulasi audio, rekayasa visual dan narasi sintesis yang disebarkan melalui platform digital lintas negara. Distribusi informasi dilakukan secara cepat dan masif sehingga publik mengalami kesulitan membedakan fakta dan rekayasa digital. *Artificial Intelligence* memberikan kemampuan untuk menciptakan simulasi visual dan audio yang menyerupai kenyataan, lalu memengaruhi pemahaman masyarakat terhadap situasi konflik internasional.³¹

Penggunaan disinformasi dalam konflik bersenjata memiliki keterkaitan dengan konsep *information warfare*. Informasi diposisikan sebagai instrumen strategis untuk membangun citra politik tertentu

³⁰ Antonio Cassese, *International Criminal Law*, Oxford University Press, Oxford, 2013, p.3-8.

³¹ Manuel Castells, *The Rise of the Network Society*, Blackwell Publishing, Oxford, 2010, p.407-409.

sekaligus melemahkan posisi lawan tanpa penggunaan kekuatan fisik secara langsung. Ruang digital berubah menjadi arena perebutan legitimasi global yang berdampak pada cara masyarakat internasional memahami tindakan militer dan posisi politik negara tertentu.³²

Kategori pertama menempatkan disinformasi sebagai persoalan tata kelola platform digital (*platform governance*). Dalam kategori ini, penyebaran informasi yang menyesatkan belum tentu memenuhi unsur tindak pidana, tetapi dapat melanggar kebijakan internal platform media sosial. Facebook, X (Twitter), YouTube dan TikTok memiliki kebijakan terkait misinformation, manipulated media dan synthetic content yang memungkinkan penghapusan konten, pelabelan informasi, pembatasan distribusi, atau penangguhan akun pengguna.

Pendekatan ini berkembang karena tidak seluruh informasi yang salah atau menyesatkan dapat dipidana. Dalam negara demokratis, kebebasan berekspresi tetap menjadi hak fundamental yang dilindungi hukum internasional, khususnya Pasal 19 International Covenant on Civil and Political Rights (ICCPR). Oleh karena itu, tindakan hukum pidana hanya dapat diterapkan apabila informasi yang disebarkan memenuhi unsur tertentu yang telah ditentukan dalam peraturan perundang-undangan. Dalam konteks konflik Iran–AS–Israel 2026, sebagian besar konten yang diperdebatkan keasliannya pada awalnya ditangani melalui mekanisme pemeriksaan fakta (*fact-checking*) dan moderasi platform sebelum memasuki ranah penegakan hukum.³³

b. Disinformasi sebagai Tindak Pidana Siber dalam Hukum Nasional

Kategori kedua menempatkan disinformasi sebagai tindak pidana siber apabila memenuhi unsur delik yang diatur dalam hukum nasional. Dalam konteks Indonesia, pengaturan mengenai penyebaran informasi elektronik saat ini mengacu pada Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

³² Joseph S. Nye, *Soft Power: The Means to Success in World Politics*, Public Affairs, New York, 2004, p.5-11.

³³ Pasal 19 International Covenant on Civil and Political Rights (ICCPR), 1966.

Pasal 28 ayat (2) menyatakan:

"Setiap Orang dengan sengaja dan tanpa hak menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi hasutan kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat berdasarkan suku, agama, ras dan antargolongan (SARA)."

Ketentuan tersebut menunjukkan bahwa tidak seluruh bentuk disinformasi dapat dipidana. Suatu informasi baru dapat dikualifikasikan sebagai tindak pidana apabila memenuhi unsur-unsur yang ditentukan undang-undang, termasuk unsur kesengajaan, sifat informasi yang dilarang dan akibat yang ditimbulkan. Dengan demikian, penggunaan deepfake atau konten sintesis berbasis *Artificial Intelligence* tidak otomatis menjadi *cybercrime* hanya karena informasi tersebut tidak sesuai dengan fakta.

c. Disinformasi sebagai Sarana yang Mendukung Kejahatan Internasional

Dalam konflik Iran–AS–Israel 2026, berbagai konten digital yang beredar lebih tepat dipahami sebagai bentuk operasi informasi (*information operation*). Kualifikasi sebagai tindak pidana hanya dapat dilakukan apabila konten tersebut memenuhi unsur delik tertentu sebagaimana diatur dalam peraturan perundang-undangan yang berlaku. Pendekatan ini sejalan dengan asas legalitas yang menghendaki bahwa tidak ada perbuatan yang dapat dipidana tanpa ketentuan hukum yang mengaturnya terlebih dahulu (*nullum crimen sine lege*).

Dalam kaitannya dengan hukum siber internasional, rujukan terhadap Convention on Cybercrime (*Budapest Convention*) 2001 juga harus dilakukan secara hati-hati. Konvensi tersebut pada dasarnya berfokus pada kejahatan terhadap sistem komputer, akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem dan kerja sama pembuktian elektronik. Sehingga oleh karena itu, disinformasi sebagai konten tidak secara otomatis termasuk dalam kategori *cybercrime* sebagaimana diatur dalam konvensi Budapest Convention. Selain itu,

Indonesia hingga saat ini belum menjadi negara pihak dalam konvensi tersebut sehingga instrumen tersebut lebih tepat digunakan sebagai referensi perkembangan hukum siber internasional dibanding sebagai dasar hukum yang mengikat secara langsung.³⁴

Dasar pertanggungjawaban pidana internasional dapat ditemukan dalam Rome Statute of the International Criminal Court. Statuta Roma memang belum mengatur disinformasi digital berbasis *Artificial Intelligence* sebagai bentuk kejahatan tersendiri. Beberapa ketentuan di dalamnya tetap membuka ruang interpretasi apabila manipulasi informasi digunakan untuk mendukung pelaksanaan kejahatan internasional.

Pasal 25 ayat (3) huruf (c) Statuta Roma menyatakan:

“For the purpose of facilitating the commission of such a crime, aids, abets or otherwise assists in its commission or its attempted commission, including providing the means for its commission.”³⁵

Analisis dari pasal statuta Roma Mahkamah Pidana Internasional tidak mengatur disinformasi digital maupun penggunaan *Artificial Intelligence* sebagai bentuk kejahatan internasional yang berdiri sendiri. Oleh karena itu, penyebaran informasi palsu dalam ruang digital tidak dapat dikualifikasikan sebagai kejahatan perang, kejahatan terhadap kemanusiaan, genosida, ataupun kejahatan agresi. Relevansi hukum pidana internasional baru muncul apabila disinformasi tersebut memiliki hubungan yang nyata dengan pelaksanaan salah satu kejahatan internasional yang menjadi yurisdiksi Mahkamah Pidana Internasional.³⁶

Dalam konteks ketentuan Pasal 25 ayat (3) huruf (c) Statuta Roma dapat menjadi dasar analisis mengenai *aiding* and *abetting*, yaitu ketika seseorang membantu, mendorong, atau menyediakan sarana yang mempermudah pelaksanaan kejahatan internasional. Namun demikian, penerapan ketentuan tersebut mensyaratkan adanya suatu hubungan yang dapat dibuktikan antara tindakan penyebaran disinformasi tersebut dengan kejahatan utama yang terjadi. Dengan kata lain,

³⁴ Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.

³⁵ Pasal 25 ayat (3) huruf (c) Rome Statute of the International Criminal Court.

³⁶ Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.

penggunaan disinformasi berbasis *Artificial Intelligence* tidak cukup hanya dibuktikan sebagai informasi yang tidak benar, tetapi juga harus dapat ditunjukkan kontribusinya terhadap pelaksanaan kejahatan internasional tertentu.

Pertanggungjawaban pidana internasional memungkinkan untuk dipertimbangkan apabila disinformasi digunakan untuk memfasilitasi serangan terhadap penduduk sipil, menghalangi bantuan kemanusiaan, memalsukan bukti pelanggaran hukum humaniter internasional, atau mendukung pelaksanaan tindakan yang termasuk dalam kategori kejahatan perang maupun kejahatan terhadap kemanusiaan. Tanpa adanya hubungan kausal yang jelas antara disinformasi dan kejahatan utama, penyebaran informasi palsu tetap berada di luar ruang lingkup yurisdiksi Mahkamah Pidana Internasional.³⁷

Penentuan pertanggungjawaban berdasarkan Pasal 25 ayat (3) huruf (c) Statuta Roma memerlukan pembuktian beberapa unsur penting, yaitu adanya yurisdiksi Mahkamah Pidana Internasional terhadap kejahatan utama, identifikasi pelaku yang dapat diatribusikan kepada individu maupun aktor tertentu, unsur kesengajaan (*mens rea*), hubungan kausal (*causal link*) antara bantuan yang diberikan dan kejahatan yang terjadi, serta standar pembuktian yang memadai (*evidentiary standard*). Oleh karena itu, keberadaan konten disinformasi semata tidak cukup untuk menimbulkan pertanggungjawaban pidana internasional tanpa adanya bukti yang menunjukkan bahwa konten tersebut secara nyata berkontribusi terhadap pelaksanaan kejahatan internasional yang menjadi yurisdiksi Mahkamah Pidana Internasional.³⁸

Kemungkinan pertanggungjawaban pidana internasional tetap terbuka apabila disinformasi berbasis *Artificial Intelligence* dapat dibuktikan:

³⁷ Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2016, p.23-31.

³⁸ James Crawford dan Martti Koskeniemi, *The Cambridge Companion to International Law*, Cambridge University Press, Cambridge, 2012, p.121-122.

1. menjadi bagian dari kejahatan internasional;
2. mendukung pelaksanaan kejahatan perang;
3. memperkuat serangan sistematis terhadap warga sipil;
4. digunakan sebagai propaganda kekerasan;
5. memiliki hubungan kausal dengan tindakan utama.

Konflik modern pada akhirnya tidak lagi berlangsung hanya di medan perang konvensional. Ruang digital telah berubah menjadi arena perebutan legitimasi, persepsi dan pengaruh global melalui manipulasi informasi berbasis Artificial Intelligence. Perubahan tersebut memperlihatkan bahwa perkembangan teknologi informasi telah menggeser pola konflik dari penggunaan kekuatan fisik menuju penguasaan arus informasi dalam ruang digital. Informasi dipergunakan untuk membangun opini publik, memperkuat propaganda politik, serta memengaruhi persepsi masyarakat internasional terhadap suatu konflik bersenjata.³⁹

Artificial Intelligence mempercepat penyebaran disinformasi melalui kemampuan menghasilkan konten digital yang realistis dan sulit diverifikasi. Teknologi deepfake, manipulasi visual, serta simulasi audio menyebabkan masyarakat mengalami kesulitan membedakan fakta dan rekayasa digital. Penyebaran informasi berlangsung secara cepat melalui media sosial dan platform digital yang bekerja menggunakan algoritma berbasis interaksi pengguna. Informasi yang bersifat provokatif dan emosional lebih mudah memperoleh perhatian publik dibanding informasi faktual sehingga propaganda digital berkembang lebih efektif dalam memengaruhi opini masyarakat.⁴⁰

Perubahan karakter konflik tersebut memperlihatkan munculnya bentuk perang baru yang tidak lagi hanya berorientasi pada penghancuran wilayah fisik, tetapi juga pada pengendalian kesadaran publik.

³⁹ Sri Wahyuni Nurdin dan Imam Fadhil Nugraha, *Op.Cit.*.

⁴⁰ Silvi Fitri Ayu dan Poetika Puspasari, *Masa Depan Demokrasi Indonesia: Penggunaan Artificial Intelligence (AI) untuk Pemilu yang Aman dan Berintegritas*, Masyarakat Indonesia, Vol.50, No.1 (2024), p.109-127.

Manipulasi informasi digunakan untuk menciptakan ketakutan massal, memperkuat polarisasi sosial, serta melemahkan kepercayaan masyarakat terhadap institusi negara dan media. Disinformasi digital pada akhirnya menjadi instrumen strategis dalam membangun dominasi politik dan psikologis dalam konflik internasional.²⁰

Perkembangan teknologi *Artificial Intelligence* juga menyebabkan meningkatnya ancaman terhadap stabilitas demokrasi dan keamanan nasional. Penyebaran hoaks, propaganda digital dan manipulasi visual dapat memengaruhi proses politik, opini masyarakat, serta legitimasi kebijakan negara. Penggunaan *Artificial Intelligence* dalam perang informasi menunjukkan bahwa ancaman digital tidak lagi bersifat individual, tetapi telah berkembang menjadi ancaman multidimensional yang memengaruhi ketahanan nasional suatu negara.⁴¹

Persoalan ini mendorong munculnya kebutuhan terhadap penguatan ketahanan informasi dan literasi digital masyarakat. Kemampuan masyarakat dalam memverifikasi informasi menjadi faktor penting dalam menghadapi disinformasi berbasis *Artificial Intelligence*. Penguatan regulasi, pengembangan teknologi forensik digital, serta kerja sama antara pemerintah, akademisi dan platform digital diperlukan untuk menghadapi perkembangan manipulasi informasi yang bergerak sangat cepat dalam ruang digital global.⁴²

C. PENUTUP

Penyebaran disinformasi berbasis *Artificial Intelligence* dalam konflik Iran–AS–Israel 2026 tidak langsung secara otomatis dapat dikualifikasikan sebagai cybercrime. Kualifikasi tersebut hanya dapat dilakukan apabila perbuatan memenuhi unsur tindak pidana tertentu yang diatur dalam hukum nasional, seperti penyebaran informasi elektronik yang menimbulkan kebencian, permusuhan, atau memiliki dampak hukum lainnya. Dalam perspektif hukum siber internasional,

⁴¹ Eddy Cahyono Sugiarto, *Ketahanan Informasi dan Literasi Digital di Era Cognitive Warfare*, Sekretariat Negara Republik Indonesia, Jakarta, 2025.

⁴² Yuwono Prianto, Albert Wibowo Santoso, Euginia Maxine Limputri, Kristinawati dan Paula Roxyana Lumban Siantar, *Disinformasi dan Krisis Kepercayaan: Turbulensi Budaya Hukum di Era Post-Truth dan Artificial Intelligence*, Titian, Vol.09, No.02 (Desember 2025).

Tomi Agi Fratama dan Priskila Kurniawati

Disinformasi Berbasis Artificial Intelligence dan Krisis Kepercayaan Publik dalam Information Warfare pada Konflik Iran–As–Israel 2026: Perspektif Hukum Siber dan Hukum Pidana Internasional

disinformasi berbasis *Artificial Intelligence* lebih tepat dipahami sebagai tantangan hukum digital yang memerlukan penguatan mekanisme pembuktian elektronik, kerja sama lintas negara dan tata kelola yang baik pada platform digital.

Dalam hukum pidana internasional, disinformasi berbasis *Artificial Intelligence* belum diakui sebagai kejahatan internasional yang berdiri sendiri. Pertanggungjawaban pidana internasional hanya dimungkinkan apabila disinformasi tersebut dapat dibuktikan berfungsi sebagai bantuan, dorongan, atau sarana yang mendukung pelaksanaan kejahatan internasional, seperti kejahatan perang, kejahatan terhadap kemanusiaan, genosida, atau agresi. Oleh karena itu, pembuktian mengenai atribusi pelaku, unsur kesalahan (*mens rea*), hubungan kausal dan keterkaitan dengan kejahatan internasional utama menjadi faktor yang menentukan dalam penetapan pertanggungjawaban pidana internasional.

DAFTAR PUSTAKA

Buku

- Brenner, Susan W. 2012. *Cybercrime and the Law: Challenges, Issues and Outcomes*. (Boston: Northeastern University Press).
- Cassese, Antonio. 2013. *International Criminal Law*. (Oxford: Oxford University Press).
- Castells, Manuel. 2010. *The Rise of the Network Society*. (Oxford: Blackwell Publishing).
- Crawford, James dan Martti Koskeniemi. 2012. *The Cambridge Companion to International Law*. (Cambridge: Cambridge University Press).
- Dinstein, Yoram. 2016. *The Conduct of Hostilities under the Law of International Armed Conflict*. (Cambridge: Cambridge University Press).
- Hiariej, Eddy O.S. 2016. *Prinsip-Prinsip Hukum Pidana*. (Yogyakarta: Cahaya Atma Pustaka).
- Maskun. 2013. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. (Jakarta: Kencana).
- Nye, Joseph S. 2004. *Soft Power: The Means to Success in World Politics*. (New York: Public Affairs).
- Sisephaputra, Bonda, dkk.. 2024. *Generative Artificial Intelligence (GenAI): Pengetahuan Dasar GenAI Beserta Penerapannya*. (Yogyakarta: Green Pustaka Indonesia).
- Sitompul, Josua. 2012. *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*. (Jakarta: Tatanusa).
- Sugiarto, Eddy Cahyono. 2025. *Ketahanan Informasi dan Literasi Digital di Era Cognitive Warfare*. (Jakarta: Sekretariat Negara Republik Indonesia).
- Suseno, Sigid. 2012. *Yurisdiksi Tindak Pidana Siber*. (Bandung: Refika Aditama).
- Wardle, Claire dan Hossein Derakhshan. 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. (Strasbourg: Council of Europe).

Publikasi

- Amaly, N. dan Armiah. *Media Digital dan Tantangan Disinformasi di Era Society 5.0*. Jurnal Ilmu Komunikasi. Vol.9. No.1 (2021).
- Amelia, Yolanda Frisky, Arfan Kaimuddin dan Hisbul Luthfi Ashsyarofi. *Pertanggungjawaban Pidana Pelaku terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake menurut Hukum Positif Indonesia*. Dinamika: Jurnal Ilmiah Ilmu Hukum. Vol.30. No.1 (2024).
- Ayu, Silvi Fitri dan Poetika Puspasari. *Masa Depan Demokrasi Indonesia: Penggunaan Artificial Intelligence (AI) untuk Pemilu yang Aman dan Berintegritas*. Masyarakat Indonesia. Vol.50. No.1 (2024).
- Ihsan, Ahmad dan Evy Nurmiati. *Akuntabilitas Profesional di Era Deepfake: Analisis Etika dan Strategi Mitigasi Penipuan Digital dalam Sistem Informasi*. Kohesi: Jurnal Multidisiplin Saintek. Vol.10. No.11 (2026).
- Iskandar, Dudi, Geri Suratno dan Didik Hariyadi Raharjo. *Construction of Digital Literacy in the 2024 Election to Stem the Flow of Hoax and Fake News*. Ekspresi dan Persepsi: Jurnal Ilmu Komunikasi. Vol.7. No.2 (Mei 2024).

Tomi Agi Fratama dan Priskila Kurniawati

Disinformasi Berbasis Artificial Intelligence dan Krisis Kepercayaan Publik dalam Information Warfare pada Konflik Iran–As–Israel 2026: Perspektif Hukum Siber dan Hukum Pidana Internasional

- Juditha, Christiany. *Artificial Intelligence dan Tantangan Disinformasi Digital di Media Sosial*. Jurnal Penelitian Komunikasi dan Opini Publik. Vol.29. No.1 (2025).
- Mongkau, Natanael Hiskia, Herlyanty Yuliana A. Bawole dan Altje Musa. *Penegakkan Hukum terhadap Penyalahgunaan Kecerdasan Buatan dengan Cara Memanipulasi Wajah Seseorang ke dalam Gambar atau Video Porno*. Lex Administratum. Vol.13. No.2 (2025).
- Nurdin, Sri Wahyuni dan Imam Fadhil Nugraha. *Ancaman Deepfake dan Disinformasi Berbasis AI: Implikasi terhadap Keamanan Siber dan Stabilitas Nasional Indonesia*. JIMR: Journal of International Multidisciplinary Research. Vol.4. No.1 (2025).
- Putri, Silvia Maharani Iskandar, Nashwa Salsabila dan Asmak U. I. Hosnah. *Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum*. Jurnal Hukum Legalita. Vol.6. No.2 (2024).
- Prianto, Yuwono, Albert Wibowo Santoso, Euginia Maxine Limputri, Kristinawati dan Paula Roxyana Lumban Siantar. *Disinformasi dan Krisis Kepercayaan: Turbulensi Budaya Hukum di Era Post-Truth dan Artificial Intelligence*. Titian: Jurnal Ilmu Humaniora. Vol.9. No.2 (Desember 2025).
- Situmeang, Bramcov Stivens, dkk.. *Pengaruh Artificial Intelligence terhadap Tingkat Kasus Deep Fake pada Selebritas di Twitter*. Device. Vol.14. No.1 (2024).
- Tulga, Ahmet Yiğitalp. *Bridging Disciplinary Gaps and Methodological Challenges in Understanding Deepfake Discourse: A Study of Turkish Reddit Posts Related to Deepfake*. Scaffold: Journal of the Institute of Comparative Studies in Literature, Arts and Culture. Vol.1. No.2 (2024).
- Tuasikal, Hendra Prayoga Hadi. *Penyebaran Konten Deepfake sebagai Tindak Pidana: Analisis Kritis terhadap Penegakan Hukum dan Perlindungan Publik di Indonesia*. Abdurrauf Law and Sharia. Vol.2. No.1 (2025).
- Wicaksono, Dimas Tri, Friyandi Prasetya dan Niken Putri Lestari. *Penegakan Hukum Terhadap Kejahatan Deepfake dalam Perspektif Hukum Positif Indonesia*. Jurnal Fakta Hukum. Vol.4. No.2 (Maret 2026).

Website

- Gstalter, M. *Obama' Voiced by Jordan Peele in PSA Video Warning about Fake Videos*. diakses dari <https://thehill.com/blogs/in-the-know/in-the-know/383525-obama-voiced-by-jordan-peelee-in-psa-video-warning-about-fake/>. diakses pada 22 Juni 2026.
- Latifa, Nur Rachmi. *Apa Itu Deepfake? Teknologi Canggih dengan Potensi Berbahaya,” Cyber Threats*. diakses dari <https://sibermate.com/hrmi/apa-itu-deepfake-teknologi-canggih-dengan-potensi-berbahaya>. diakses pada 22 Juni 2026.

Sumber Hukum

- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

International Covenant on Civil and Political Rights (ICCPR), 1966.
Rome Statute of the International Criminal Court, 1998.
Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.
International Law Commission. Articles on Responsibility of States for
Internationally Wrongful Acts. New York: United Nations, 2001.

Sumber Lain

Asosiasi Penyelenggara Jasa Internet Indonesia. 2025. *Survei Penetrasi Internet Indonesia 2025*. Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia.

