Volume 14 No 2 (2026)
E- ISSN : 2580-2461
P-ISSN: 2339-1693
https://ejournal.upbatam.ac.id/index.php/cahayakeadilan

JURNAL CAHAYA KEADILAN

TANTANGAN HUKUM INTERNASIONAL DALAM MENGATUR TEKNOLOGI DEEPFAKE: STUDI KASUS PENYEBARAN DISINFORMASI DALAM KONFLIK RUSIA-UKRAINA

Johana Jelita Hutasoit
Program Studi Ilmu Hukum, Fakultas Sosial dan Humanoira, Universitas Putra Batam
Email: johanajelitaqueen@gmail.com

Diki Zukriadi[3]
Program Studi Ilmu Hukum, Fakultas Sosial dan Humanoira, Universitas Putra Batam
Email: diki@puterabatam.ac.id

Abstrak

Perkembangan teknologi digital, khususnya teknologi deepfake, telah menciptakan tantangan baru bagi hukum internasional, terutama dalam konteks konflik bersenjata modern. Pokok permasalahan dalam penelitian ini adalah bagaimana hukum internasional merespons penyebaran disinformasi berbasis deepfake dalam konflik Rusia-Ukraina dan sejauh mana kerangka hukum yang ada mampu mengatasi ancaman tersebut. Tujuan penelitian ini adalah untuk menganalisis penggunaan deepfake dalam konflik Rusia-Ukraina, mengidentifikasi celah dalam regulasi hukum internasional, serta merumuskan rekomendasi strategis guna memperkuat tata kelola disinformasi digital global.Metode yang digunakan dalam penelitian ini adalah pendekatan kualitatif-deskriptif dengan metode studi kasus terhadap konflik Rusia-Ukraina. Data dikumpulkan melalui kajian literatur, analisis dokumentasi, dan telaah terhadap insiden penyebaran konten deepfake yang berdampak signifikan terhadap persepsi publik dan stabilitas politik.Hasil penelitian menunjukkan bahwa regulasi hukum internasional saat ini, termasuk hukum humaniter internasional dan hak asasi manusia internasional, belum memiliki ketentuan yang secara khusus mengatur fenomena deepfake. Ketiadaan definisi legal yang jelas, lemahnya mekanisme atribusi terhadap pelaku, serta keterbatasan kerja sama antarnegara menjadi hambatan utama dalam upaya penanggulangan disinformasi digital di ranah global.Kesimpulan dari penelitian ini menegaskan perlunya pembaruan norma hukum internasional, pembentukan konvensi khusus tentang disinformasi digital, pendirian badan internasional penanggulangan deepfake, dan penguatan literasi digital global. Sinergi antarnegara, sektor swasta, dan masyarakat sipil menjadi kunci dalam membangun sistem perlindungan informasi yang aman dan bertanggung jawab di era digital.

Kata kunci: *deepfake, disinformasi, hukum internasional, konflik Rusia-Ukraina, teknologi digital, hukum humaniter.*

I. Pendahuluan

I.1 Latar Belakang

Perkembangan teknologi digital di era modern telah memberikan dampak besar terhadap berbagai bidang kehidupan manusia, termasuk dalam ranah politik, keamanan, dan hukum internasional. Salah satu inovasi teknologi yang kini menjadi sorotan dunia adalah teknologi deepfake**,** yakni teknologi

berbasis kecerdasan buatan (Artificial Intelligence) yang memungkinkan manipulasi gambar, video, dan suara secara realistis sehingga sulit dibedakan dari konten asli. Meski dapat dimanfaatkan untuk kepentingan positif di bidang seni, hiburan, dan edukasi, kehadiran teknologi ini juga menimbulkan ancaman serius, terutama dalam konteks penyebaran disinformasi yang dapat memicu ketegangan sosial dan konflik antarnegara.Salah satu kasus nyata yang memperlihatkan penyalahgunaan teknologi deepfake adalah konflik Rusia-Ukraina**,** di mana teknologi ini digunakan sebagai instrumen perang informasi Video-video palsu yang menampilkan tokoh penting, seperti Presiden Ukraina Volodymyr Zelenskyy, dengan narasi yang memerintahkan pasukan untuk menyerah telah tersebar luas di berbagai platform digital. Penyebaran konten manipulatif ini tidak hanya menimbulkan kebingungan di masyarakat, tetapi juga berpotensi memengaruhi stabilitas politik, melemahkan posisi diplomatik negara di kancah internasional, hingga menghambat upaya perdamaian. Fenomena ini memperlihatkan bahwa disinformasi berbasis deepfake menjadi senjata strategis dalam konflik modern yang dapat mengancam keamanan regional maupun tatanan hukum internasional. Dalam kerangka hukum internasional, fenomena deepfake menimbulkan tantangan serius karena hingga saat ini belum terdapat aturan hukum yang secara spesifik mengatur teknologi tersebut, baik dalam hukum humaniter internasional (HHI) maupun hukum hak asasi manusia internasional**.** Prinsip-prinsip hukum humaniter seperti perlindungan terhadap warga sipil dan larangan penggunaan taktik penyesatan.

II. Metode Penelitian

Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus, karena permasalahan yang diangkat terkait dengan penyebaran disinformasi berbasis teknologi deepfake dalam konflik Rusia–Ukraina memerlukan pemahaman mendalam terhadap konteks, motif, dan dampaknya. Pendekatan ini dipilih agar peneliti dapat mengeksplorasi secara menyeluruh tantangan hukum internasional yang muncul sebagai akibat dari perkembangan teknologi manipulatif.Jenis penelitian ini bersifat normatif-empiris, di mana analisis dilakukan tidak hanya pada ketentuan hukum positif yang berlaku (normatif), tetapi juga pada praktik nyata yang terjadi dalam peristiwa penyebaran deepfake di lapangan (empiris), seperti dalam konflik Rusia–Ukraina. Dengan demikian, penelitian ini berusaha menjembatani antara teori hukum internasional dan dinamika teknologi digital dalam konteks konflik modern.

2.2. Teknik dan Metode Pengumpulan Data

Untuk memperoleh data yang relevan dan komprehensif, penelitian ini menggunakan tiga teknik utama dalam pengumpulan data, yaitu:

1. **Studi Pustaka**

Peneliti melakukan penelusuran dan kajian mendalam terhadap sumber-sumber hukum internasional primer dan sekunder, antara lain:

- Piagam Perserikatan Bangsa-Bangsa (PBB)
- Konvensi Jenewa dan Protokol Tambahannya
- Laporan dan dokumen resmi lembaga internasional seperti Human Rights Watch, ICRC, dan UNHRC
- Artikel ilmiah, jurnal akademik, dan buku-buku hukum siber, hukum humaniter, dan etika digital
- Tallinn Manual 2.0 tentang Hukum Internasional dalam Operasi Siber

2. **Dokumentasi dan Telaah Data Digital**

Peneliti mengakses dan menganalisis berbagai video, gambar, dan konten berbasis teknologi deepfake yang beredar selama konflik Rusia–Ukraina, khususnya insiden yang melibatkan manipulasi citra tokoh publik, seperti video palsu Presiden Volodymyr Zelenskyy. Data ini diperoleh dari sumber berita terpercaya, platform media sosial, dan arsip digital.

3. **Telaah Kasus dan Laporan Investigatif**

Studi kasus yang dikaji berasal dari dokumentasi laporan investigatif tentang penyebaran konten deepfake yang memiliki pengaruh signifikan terhadap persepsi publik, keamanan, dan kebijakan internasional. Kasus dipilih secara purposif berdasarkan relevansi dan signifikansi terhadap tujuan.

III. Hasil Penelitian Dan Pembahasan

Penggunaan teknologi deepfake dalam konflik Rusia–Ukraina tampil sebagai instrumen strategis perang informasi. Konten deepfake digunakan untuk menyebarkan disinformasi dengan tujuan mengacaukan persepsi publik, menimbulkan kebingungan, dan melemahkan moral pihak lawan.Salah satu contoh menonjol adalah video palsu Presiden Volodymyr Zelenskyy yang tampak memberi perintah kepada tentaranya untuk menyerah. Video ini menyebar di berbagai platform media sosial dan sempat dipercaya oleh sebagian masyarakat sebelum dikonfirmasi sebagai palsu. Taktik ini menandai bahwa deepfake

tidak hanya berfungsi sebagai konten digital, tetapi juga sebagai senjata psikologis dalam konflik bersenjata.Selain itu, penggunaan akun bot otomatis dan kampanye sistematis melalui media sosial menunjukkan bahwa penyebaran deepfake tidak terjadi secara sporadis, melainkan dirancang secara terkoordinasi sebagai bagian dari operasi perang informasi lintas negara. Tantangan hukum internasional dalam mengatur penyebaran deepfake bersumber dari tiga aspek utama:

1. Ketiadaan definisi legal internasional yang jelas mengenai deepfake. Tanpa definisi yang disepakati secara global, sulit bagi negara atau lembaga internasional untuk menentukan apakah suatu konten deepfake merupakan pelanggaran hukum internasional.
2. Kesulitan atribusi pelaku. Karena penyebaran deepfake sering kali melibatkan teknologi pengaburan identitas, seperti VPN, jaringan bot, dan IP masking, maka proses penetapan pelaku (baik negara maupun aktor non-negara) menjadi sangat sulit, padahal dalam hukum internasional, atribusi merupakan syarat utama untuk pertanggungjawaban hukum.
3. Belum adanya rezim hukum siber internasional yang mengikat. Meskipun ada dokumen-dokumen seperti *Tallinn Manual*, dokumen tersebut tidak memiliki kekuatan hukum mengikat. Akibatnya, tidak ada mekanisme sanksi internasional yang dapat digunakan secara langsung untuk menindak penyebar deepfake lintas negara.
4. Keterbatasan kapasitas negara berkembang, baik dalam deteksi teknologi deepfake maupun dalam pembentukan kebijakan hukum domestik yang relevan.

Kerangka hukum internasional yang berlaku saat ini—termasuk hukum humaniter internasional (HHI) dan hukum hak asasi manusia internasional (HAM Internasional)—belum secara langsung dan eksplisit merespons fenomena deepfake.

- Dalam konteks HHI, prinsip-prinsip seperti perlindungan terhadap warga sipil, larangan taktik menyesatkan yang tidak perlu, dan larangan terhadap senjata non-konvensional yang membahayakan secara luas, dapat diinterpretasikan untuk mencakup penggunaan deepfake. Namun, tidak ada pasal khusus yang secara eksplisit menyebutkan disinformasi digital sebagai pelanggaran.
- Dalam HAM internasional, penyebaran deepfake dapat melanggar hak atas informasi yang benar, hak atas keamanan, serta hak atas reputasi dan martabat pribadi. Namun kembali, ketiadaan standar eksplisit menyebabkan lemahnya daya paksa hukum tersebut.

Kesimpulannya, hukum internasional saat ini bersifat reaktif, belum proaktif, dan lebih banyak bergantung pada interpretasi luas terhadap prinsip yang sudah ada

Berdasarkan analisis isi terhadap berbagai dokumen hukum dan insiden penyebaran deepfake, dapat disimpulkan bahwa:

- Ketiadaan definisi legal tentang deepfake menyebabkan ketidaksamaan persepsi antarnegara dalam menilai status hukum suatu konten manipulatif. Akibatnya, tindakan penyebaran deepfake tidak dapat diklasifikasikan dengan jelas sebagai pelanggaran hukum internasional.
- Kompleksitas teknologi deepfake — termasuk kemampuan menyamarkan identitas pelaku melalui IP masking, bot otomatis, dan jaringan terdistribusi — menyulitkan proses atribusi dan pembuktian dalam sistem hukum internasional. Hal ini bertentangan dengan prinsip atribusi yang menjadi dasar pertanggungjawaban negara (state responsibility).

Penelitian ini menguatkan argumen yang telah dikemukakan oleh Chesney & Citron (2019) mengenai "*Looming Challenge for Democracy*" yang menyatakan bahwa deepfake bukan hanya ancaman terhadap privasi, tetapi juga terhadap demokrasi dan stabilitas global. Selain itu, hasil penelitian ini sejalan dengan konsep "*Information Warfare*" yang dikembangkan dalam Tallinn Manual 2.0, yang menyebutkan bahwa operasi siber yang menyesatkan publik sipil dalam masa konflik dapat dianggap sebagai pelanggaran terhadap hukum perang jika dampaknya menyerupai tindakan militer langsung. Namun, penelitian ini melampaui kerangka teori sebelumnya dengan memasukkan aspek etika digital dan tata kelola global sebagai bagian dari reformasi hukum internasional yang lebih menyeluruh. Dengan demikian, temuan ini memperluas pendekatan normatif hukum humaniter klasik menjadi lebih adaptif terhadap teknologi.

Salah satu kontribusi teoritis dari penelitian ini adalah usulan modifikasi terhadap konsep kombatan dalam hukum humaniter internasional. Dalam konteks digital, pelaku penyebaran disinformasi yang memiliki dampak strategis terhadap keamanan negara seharusnya diakui sebagai "digital combatant" — yaitu individu atau entitas yang secara aktif terlibat dalam operasi manipulatif berteknologi tinggi dalam situasi konflik. Konsep ini akan memperluas cakupan subjek hukum perang dan membuka jalan bagi:

- Pemberlakuan prinsip distinction dalam ruang digital (membedakan antara konten sipil dan konten perang);
- Pengaturan status hukum aktor non-negara digital;
- Penerapan sanksi internasional terhadap pelaku disinformasi yang menimbulkan dampak serupa senjata non-fisik (cyber-weaponized content).

Model ini memperkuat bahwa penyebaran deepfake bukan sekadar pelanggaran etik atau privasi, melainkan dapat menjadi bentuk agresi digital yang harus direspons secara hukum dan diplomatik.

IV. Simpulan Dan Saran
4.1 Simpulan

Berdasarkan hasil penelitian tentang tantangan hukum internasional dalam mengatur teknologi deepfake, khususnya dalam konteks konflik Rusia–Ukraina, dapat disimpulkan bahwa fenomena deepfake telah bertransformasi menjadi instrumen strategis dalam perang informasi modern. Penggunaan konten manipulatif yang menyasar persepsi publik dan stabilitas politik menunjukkan bahwa deepfake bukan sekadar persoalan etika atau privasi, melainkan telah menjadi ancaman nyata bagi keamanan global dan ketertiban hukum internasional. Salah satu bentuk nyata penyalahgunaan teknologi ini adalah penyebaran video palsu yang menampilkan Presiden Ukraina Volodymyr Zelenskyy seolah-olah memerintahkan pasukan untuk menyerah, yang berdampak signifikan terhadap moral publik dan diplomasi internasional. Tindakan semacam ini memperlihatkan bagaimana teknologi deepfake dimanfaatkan sebagai senjata psikologis dalam konflik bersenjata.

Dalam kerangka hukum internasional saat ini, ditemukan sejumlah tantangan fundamental dalam menghadapi ancaman deepfake. Pertama, belum adanya definisi hukum internasional yang baku dan diakui secara global mengenai apa itu deepfake menyulitkan proses klasifikasi dan penindakan terhadap konten manipulatif tersebut. Kedua, proses atribusi pelaku penyebaran deepfake sangat kompleks akibat kecanggihan teknologi yang dapat menyembunyikan identitas pelaku melalui berbagai metode digital, seperti IP masking dan bot otomatis. Ketiga, ketiadaan rezim hukum siber internasional yang bersifat mengikat menyebabkan lemahnya mekanisme penegakan hukum dan sanksi bagi pelaku penyebaran disinformasi lintas negara. Selain itu, keterbatasan kapasitas negara-negara berkembang dalam deteksi dan pengaturan hukum domestik terkait disinformasi digital turut memperparah situasi.

Adapun hukum humaniter internasional dan hukum hak asasi manusia internasional sejauh ini hanya memberikan ketentuan umum yang belum secara eksplisit mengatur tentang fenomena deepfake. Meskipun prinsip-prinsip dasar seperti perlindungan terhadap warga sipil, larangan taktik menyesatkan, serta hak atas informasi yang benar dapat diinterpretasikan untuk mencakup penyebaran disinformasi digital, absennya norma khusus membuat hukum internasional cenderung reaktif dan bergantung pada tafsir luas semata. Hal ini menunjukkan adanya kekosongan hukum (legal gap) yang berpotensi dimanfaatkan oleh aktor negara maupun non-negara untuk melakukan agresi informasi tanpa konsekuensi hukum yang tegas.

Oleh karena itu, penelitian ini menegaskan perlunya reformasi hukum internasional strategis dapat dikenakan tanggung jawab hukum setara dengan pelaku konvensional secara sistemik untuk merespons tantangan deepfake dan disinformasi digital. Rekomendasi strategis yang ditawarkan meliputi pembentukan konvensi internasional khusus tentang disinformasi digital yang mencakup definisi legal deepfake dan mekanisme atribusi yang jelas, pendirian badan internasional di bawah PBB yang berwenang menangani penyebaran deepfake secara lintas negara, serta penguatan literasi digital global untuk meningkatkan ketahanan masyarakat terhadap konten manipulatif. Selain itu, diusulkan pula modifikasi konsep hukum humaniter internasional melalui pengenalan status hukum baru bagi pelaku agresi digital atau *digital combatant*, sehingga aktor siber yang menyebarkan disinformasi berskala dalam konflik bersenjata. Dengan demikian, penelitian ini tidak hanya memetakan permasalahan hukum yang ada, tetapi juga memberikan kontribusi konseptual bagi pengembangan hukum internasional yang lebih adaptif, progresif, dan responsif terhadap tantangan teknologi digital di masa depan

DAFTAR PUSTAKA

Brookings Institution. (2022). *The future of war: Information warfare in the digital age*. Retrieved from https://www.brookings.edu/research/the-future-of-war-information-warfare

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820. https://doi.org/10.2139/ssrn.3213954

Geneva Conventions. (1949). *Geneva Conventions of 12 August 1949 and their Additional Protocols*. International Committee of the Red Cross.

Human Rights Watch. (2022). *Ukraine: Civilian casualties from apparent Russian cluster munition attacks*. Retrieved from https://www.hrw.org/news/2022/02/28/ukraine-civilian-casualties

International Committee of the Red Cross (ICRC). (2022). *International humanitarian law and cyber operations during armed conflicts*.

Kurbalija, J. (2016). *An introduction to Internet governance* (7th ed.). Geneva: DiploFoundation.

Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017). Cambridge University Press. https://doi.org/10.1017/9781316822524 z

United Nations Human Rights Council (UNHRC). (2022). *Report of the Independent International Commission of Inquiry on Ukraine*. A/HRC/50/CRP.1.

United Nations. (1945). *Charter of the United Nations and Statute of the International Court of Justice*. San Francisco: United Nations

Wheeler, D. (2020). *Cyber conflict and international humanitarian law: New challenges in the digital battlespace*. London: Routledge