

BAB IV

PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan dalam bab-bab sebelumnya mengenai penggunaan teknologi *deepfake* dalam konflik bersenjata, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Pengaturan *Deepfake* sebagai Metode Berperang dalam Hukum Internasional yang mencakup *Konvensi Den Haag* 1907, Piagam PBB 1945, Protokol Tambahan I 1977, serta interpretasi komprehensif dalam *Tallinn Manual 2.0*. Teknologi *deepfake* secara yuridis diklasifikasikan sebagai Metode Berperang Non-Kinetik dalam domain peperangan informasi siber. Pengaturan *deepfake* dalam hukum internasional *deepfake* ditentukan melalui ambang batas penerapan prinsip Itikad Baik (*Good Faith*) sebagaimana mandat Pasal 2 ayat (2) Piagam PBB, di mana teknologi ini diakui sebagai Muslihat Perang (*Ruses of War*) yang sah apabila digunakan untuk tujuan penyesatan strategi, kamuflase informasi, atau memengaruhi moral lawan tanpa melanggar norma hukum internasional lainnya Pasal 24 *Konvensi Den Haag* 1907, Pasal 37 ayat (2) Protokol Tambahan I 1977, dan Rule 123 *Tallinn Manual 2.0*). Namun, *deepfake* bertransformasi menjadi metode yang dilarang (ilegal) dan dikategorikan sebagai kejahatan Pengkhianatan (*Perfidy*) berdasarkan Pasal 37 ayat (1) Protokol Tambahan I 1977, serta *Rule 122 Tallinn Manual 2.0*, apabila manipulasi audio-visual tersebut sengaja digunakan untuk mengeksploitasi kepercayaan musuh terhadap status perlindungan hukum internasional seperti memalsukan niat untuk menyerah atau menyamar sebagai warga sipil guna membunuh,

melukai, atau menangkap lawan melalui penipuan yang bersifat khianat..

2. Analisis Yuridis penggunaan teknologi *deepfake* dalam konflik Rusia-Ukraina, seperti pada kasus video palsu Presiden Zelenskyy, Presiden Putin dan Jenderal Zaluzhnyi, merupakan manifestasi modern dari metode peperangan yang secara yuridis dikategorikan sebagai muslihat perang (*ruses of war*) yang diperbolehkan dalam hukum internasional yang sesuai dengan aturan pada pasal 24 konvensi den haag 1907, pasal 37 (2) Protokol Tambahan I 1977 dan pasal 123 Tallin Manual 2.0. Oleh karena itu tindakan penggunaan *deepfake* dalam kasus ini dianggap sah karena bertujuan untuk menyesatkan persepsi strategis dan kewaspadaan militer lawan tanpa mengeksploitasi itikad baik atau perlindungan khusus yang diatur dalam Hukum Internasional, sehingga tidak memenuhi unsur pengkhianatan (*perfidy*). Meskipun demikian, penggunaan *deepfake* tetap memiliki batasan legalitas yang ketat, di mana manipulasi digital tersebut akan menjadi ilegal jika digunakan untuk menciptakan kepercayaan palsu terhadap status yang dilindungi dengan maksud membunuh atau melukai musuh.

B. Saran

Sejalan dengan kesimpulan yang telah dikemukakan di atas, peneliti merumuskan beberapa saran yang diharapkan dapat menjadi kontribusi positif bagi pengembangan hukum internasional dan kebijakan pertahanan di masa depan:

1. Perlu adanya pembentukan Regulasi Internasional Khusus AI dalam Konflik Bersenjata karena adanya keterbatasan pada instrumen hukum klasik seperti Konvensi Den Haag 1907 dan Protokol Tambahan I 1977 dalam menjangkau dimensi siber, disarankan kepada komunitas internasional untuk menginisiasi kodifikasi norma baru dalam bentuk protokol tambahan

khusus atau *interpretative guidance* yang bersifat mengikat. Regulasi ini harus mampu memberikan parameter teknis dan hukum yang definitif mengenai ambang batas (*threshold*) penggunaan kecerdasan buatan. Fokus utamanya adalah memperjelas garis demarkasi antara manipulasi digital sebagai Muslihat Perang (*Ruses of War*) yang legal dengan tindakan Pengkhianatan (*Perfidy*) digital. Hal ini penting guna memastikan bahwa prinsip itikad baik (*good faith*) tetap terjaga dan tidak terjadi kekosongan hukum (*legal gap*) ketika teknologi *deepfake* digunakan untuk memalsukan identitas otoritas militer maupun sipil dalam situasi konflik.

2. Perlu adanya penguatan Prinsip Pembedaan (*Distinction*) dan Mekanisme Atribusi Siber sebagai penegakan hukum dalam kasus *deepfake* di konflik Rusia-Ukraina, agar setiap negara secara tegas mengintegrasikan Prinsip Pembedaan (*Distinction*) ke dalam doktrin peperangan siber mereka. Negara wajib memastikan bahwa penggunaan *deepfake* tidak dieksploitasi untuk menysasar populasi sipil atau merusak objek-objek sipil yang dilindungi hukum internasional. Lebih lanjut, diperlukan penguatan standar Atribusi dan Tanggung Jawab Negara (*State Responsibility*) melalui penerapan prinsip *cyber due diligence*. Negara harus memiliki kewajiban hukum untuk mencegah, mendeteksi, dan menghentikan operasi informasi berbasis AI yang bersifat merusak dari wilayah kedaulatannya. Hal ini harus didukung dengan pembentukan konsorsium verifikasi digital internasional yang independen guna mempermudah proses pembuktian forensik digital dan identifikasi aktor intelektual di balik serangan *deepfake* yang melanggar kedaulatan negara lain