JRH
JURNAL REALITAS HUKUM
P-ISSN -
E-ISSN -
https://jurnal.prestasiku.org
VOLUME 2
NO. 2
MARET 2026

TANTANGAN HUKUM DALAM PENYALAHGUNAAN TEKNOLOGI DEEPFAKE ARTIFICIAL INTELLIGENCE DI INDONESIA

Aan Tirta Gandana[1], Agus Hendrayana[2], Dainsyah[3], Deny M. Ramdhany[4], Jeny Mellysa Ariyanti[5]

Program Studi Magister Ilmu Hukum, Universitas Langlangbuana, Email: banthar76@gmail.com
Program Studi Magister Ilmu Hukum, Universitas Langlangbuana, Email: agus76hendra@gmail.com
Program Studi Magister Ilmu Hukum, Universitas Langlangbuana, Email: dainsyah@gmail.com
Program Studi Magister Ilmu Hukum, Universitas Langlangbuana, Email: denimorand@gmail.com
Program Studi Magister Ilmu Hukum, Universitas Langlangbuana, Email: melyyyjenyy@gmail.com

ABSTRAK

Perkembangan teknologi Artificial Intelligence (AI), khususnya deepfake, telah membawa perubahan signifikan dalam kehidupan digital masyarakat. Teknologi ini mampu menghasilkan manipulasi audio dan visual yang sangat realistis sehingga sulit dibedakan dari konten asli. Meskipun memiliki manfaat dalam industri kreatif dan komunikasi, penyalahgunaan deepfake menimbulkan ancaman serius terhadap privasi, keamanan, serta kepercayaan publik. Penelitian ini bertujuan untuk menganalisis bentuk penyalahgunaan teknologi deepfake di dunia maya serta mengkaji pengaturan hukum di Indonesia dalam mengantisipasi permasalahan tersebut. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa deepfake telah disalahgunakan dalam berbagai bentuk seperti penipuan digital, iklan palsu, pencurian identitas, dan penyebaran disinformasi. Regulasi di Indonesia seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Konsumen, dan Undang-Undang Perlindungan Data Pribadi belum secara eksplisit mengatur deepfake. Oleh karena itu, diperlukan penguatan regulasi khusus, peningkatan literasi digital masyarakat, serta pengembangan teknologi deteksi deepfake untuk meminimalisir dampak negatifnya.

Kata kunci: Deepfake, Kecerdasan Buatan, Kejahatan Siber, Tantangan Hukum

ABSTRACT

The development of Artificial Intelligence (AI), particularly deepfake technology, has significantly transformed digital communication. Deepfake enables the creation of highly realistic manipulated audio and video content that is difficult to distinguish from authentic media. While it offers benefits in creative industries, its misuse poses serious risks to privacy, security, and public trust. This study aims to analyze the misuse of deepfake technology in cyberspace and examine the adequacy of Indonesia's legal framework in addressing such issues. The research uses a normative juridical method with statutory and conceptual approaches through library research. The findings reveal that deepfake is widely used for digital fraud, fake advertising, identity theft, and misinformation. Existing regulations such as the ITE Law, Consumer Protection Law, and Personal Data

Protection Law have not explicitly regulated deepfake. Therefore, stronger regulations, digital literacy improvement, and deepfake detection technologies are urgently needed.

Keywords: Deepfake, Artificial Intelligence, Cybercrime, Legal Challenges

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) dalam beberapa dekade terakhir telah membawa perubahan yang sangat signifikan dalam berbagai aspek kehidupan masyarakat modern. Transformasi digital tidak hanya mengubah cara manusia berkomunikasi, tetapi juga mempengaruhi pola interaksi sosial, ekonomi, politik, dan budaya. Internet dan media sosial memungkinkan penyebaran informasi secara cepat, masif, dan tanpa batas geografis. Namun, di balik kemudahan tersebut, perkembangan teknologi juga memunculkan berbagai bentuk kejahatan baru di dunia maya (cyber crime) yang semakin kompleks dan sulit dikendalikan.

Salah satu inovasi teknologi yang berkembang pesat adalah Artificial Intelligence (AI), khususnya teknologi deepfake. Deepfake merupakan teknologi berbasis kecerdasan buatan yang mampu memanipulasi konten digital berupa video, gambar, dan audio sehingga terlihat sangat realistis dan sulit dibedakan dari aslinya. Teknologi ini bekerja dengan memanfaatkan algoritma machine learning, terutama Generative Adversarial Networks (GANs), yang memungkinkan sistem komputer mempelajari pola wajah, suara, dan gerakan seseorang untuk kemudian merekonstruksi atau memalsukan konten digital secara akurat.

Pada dasarnya, teknologi deepfake memiliki potensi positif yang cukup besar, terutama dalam bidang industri kreatif seperti perfilman, periklanan, pendidikan, dan hiburan. Deepfake dapat digunakan untuk efek visual, rekonstruksi tokoh sejarah, hingga pengembangan konten interaktif. Namun, di sisi lain, teknologi ini juga membawa potensi risiko yang sangat serius apabila disalahgunakan. Kemudahan akses terhadap perangkat lunak deepfake serta meningkatnya kualitas hasil manipulasi menjadikan teknologi ini sebagai alat yang berbahaya dalam berbagai bentuk kejahatan siber.

Fenomena penyalahgunaan deepfake saat ini semakin marak terjadi, baik di tingkat global maupun nasional. Salah satu bentuk yang paling sering ditemukan adalah penggunaan deepfake dalam iklan digital yang mencatut identitas tokoh publik tanpa izin. Dalam praktiknya, pelaku menggunakan wajah dan suara tokoh terkenal, seperti pejabat publik, tenaga medis, atau selebritas, untuk mempromosikan produk tertentu. Konten tersebut seringkali mengandung informasi yang menyesatkan dan bertujuan untuk mempengaruhi kepercayaan masyarakat demi keuntungan ekonomi.

Selain dalam bidang periklanan, deepfake juga digunakan dalam berbagai bentuk kejahatan lain seperti penipuan finansial, pencurian identitas, penyebaran hoaks, hingga manipulasi opini publik. Bahkan, dalam konteks yang lebih luas, deepfake berpotensi digunakan sebagai alat propaganda politik dan disinformasi yang dapat mengganggu stabilitas sosial dan keamanan nasional. Kemampuan deepfake dalam menciptakan realitas palsu (synthetic reality) menjadi ancaman serius terhadap kepercayaan publik terhadap informasi digital.

Di Indonesia, perkembangan teknologi deepfake menunjukkan tren yang semakin meningkat seiring dengan pesatnya penggunaan media sosial dan platform digital. Masyarakat yang belum sepenuhnya memiliki literasi digital yang memadai menjadi rentan terhadap manipulasi informasi berbasis deepfake. Hal ini diperparah dengan belum optimalnya sistem pengawasan dan penegakan hukum terhadap konten digital yang beredar di ruang siber.

Dari perspektif hukum, penyalahgunaan teknologi deepfake menimbulkan berbagai persoalan yang kompleks, terutama terkait dengan perlindungan data pribadi, pencemaran nama baik, penipuan, serta perlindungan konsumen. Meskipun Indonesia telah memiliki beberapa regulasi yang relevan, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Konsumen, dan Undang-Undang Perlindungan Data Pribadi, namun regulasi tersebut belum secara spesifik mengatur mengenai deepfake. Akibatnya, terdapat kekosongan norma (legal gap) dalam mengantisipasi dan menindak penyalahgunaan teknologi ini secara komprehensif.

Kondisi tersebut menunjukkan adanya kesenjangan antara perkembangan teknologi yang sangat cepat dengan kesiapan hukum dalam mengaturnya. Hukum seringkali tertinggal dibandingkan dengan inovasi teknologi, sehingga menimbulkan tantangan baru bagi pemerintah dan aparat penegak hukum dalam memberikan perlindungan yang optimal kepada masyarakat. Oleh karena itu, diperlukan kajian yang mendalam mengenai bagaimana bentuk penyalahgunaan teknologi deepfake serta bagaimana kerangka hukum di Indonesia dapat merespons fenomena tersebut.

Berdasarkan latar belakang tersebut, penelitian ini menjadi penting untuk dilakukan guna menganalisis secara komprehensif bentuk-bentuk penyalahgunaan deepfake di dunia maya serta mengevaluasi pengaturan hukum yang berlaku di Indonesia. Dengan demikian, diharapkan penelitian ini dapat memberikan kontribusi dalam pengembangan kebijakan hukum yang adaptif terhadap kemajuan teknologi serta mampu melindungi masyarakat dari dampak negatif penggunaan deepfake.

METODE PENELITIAN

1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan jenis penelitian yuridis normatif, yaitu penelitian hukum yang dilakukan dengan cara mengkaji dan menganalisis norma-norma hukum yang terdapat dalam peraturan perundang-undangan, putusan pengadilan, serta doktrin atau pendapat para ahli hukum. Penelitian yuridis normatif berfokus pada hukum sebagai suatu sistem norma yang bertujuan untuk menemukan asas, prinsip, serta kaidah hukum yang relevan dengan permasalahan yang diteliti, khususnya terkait penyalahgunaan teknologi deepfake dalam perspektif hukum di Indonesia.

Adapun pendekatan yang digunakan dalam penelitian ini meliputi:

a) Pendekatan Perundang-undangan (statute approach), yaitu dengan menelaah Pendekatan ini dilakukan dengan menelaah berbagai peraturan perundang-undangan yang berkaitan dengan permasalahan penelitian, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Perlindungan Konsumen, serta Peraturan Pemerintah terkait perdagangan melalui sistem elektronik. Pendekatan ini bertujuan untuk mengetahui sejauh mana hukum positif di Indonesia mengatur penyalahgunaan teknologi deepfake.
b) Pendekatan Konseptual (conceptual approach), yaitu dengan mengkaji konsep-konsep Pendekatan ini dilakukan dengan mengkaji konsep-konsep hukum yang berkembang dalam literatur akademik, seperti konsep kejahatan siber (cyber crime), perlindungan data pribadi, serta tanggung jawab hukum dalam penggunaan teknologi digital. Pendekatan ini digunakan untuk membangun kerangka teoritis dalam menganalisis fenomena deepfake.

2. Sifat Penelitian

Penelitian ini bersifat **deskriptif-analitis**, yaitu penelitian yang bertujuan untuk menggambarkan secara sistematis, faktual, dan akurat mengenai fenomena penyalahgunaan teknologi deepfake, kemudian dianalisis untuk memperoleh pemahaman yang komprehensif mengenai permasalahan hukum yang timbul. Melalui pendekatan ini, penulis tidak hanya mendeskripsikan fakta, tetapi juga melakukan analisis terhadap kesenjangan antara norma hukum yang berlaku dengan praktik yang terjadi di masyarakat.

3. Sumber dan Jenis Bahan Hukum

Bahan hukum yang digunakan dalam penelitian ini terdiri atas:

a) Bahan hukum primer, Yaitu bahan hukum yang memiliki kekuatan mengikat, berupa peraturan perundang-undangan yang relevan dengan penelitian, antara lain:
   1. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik
   2. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
   3. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen
   4. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik

b) Bahan hukum sekunder, Yaitu bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, seperti buku teks hukum, jurnal ilmiah, hasil penelitian, artikel akademik, serta pendapat para ahli yang berkaitan dengan deepfake, artificial intelligence, dan cyber crime.

c) Bahan hukum tersier, Yaitu bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus hukum, ensiklopedia, serta sumber informasi dari media massa yang relevan dengan penelitian.

4. Teknik Pengumpulan Bahan Hukum

Teknik pengumpulan bahan hukum dalam penelitian ini dilakukan melalui studi kepustakaan (library research), yaitu dengan cara menginventarisasi, mengkaji, dan menganalisis berbagai literatur hukum yang relevan. Pengumpulan data dilakukan dengan menelusuri peraturan perundang-undangan, buku, jurnal ilmiah, serta sumber lain yang berkaitan dengan penyalahgunaan teknologi deepfake dan pengaturannya dalam hukum Indonesia.

5. Teknik Analisis Bahan Hukum

Analisis bahan hukum dilakukan secara **kualitatif**, yaitu dengan menafsirkan dan mengkaji bahan hukum yang telah dikumpulkan secara sistematis untuk memperoleh kesimpulan yang relevan dengan permasalahan penelitian. Proses analisis dilakukan dengan cara menghubungkan antara norma hukum yang berlaku dengan fenomena penyalahgunaan deepfake yang terjadi di masyarakat.

6. Teknik Penarikan Kesimpulan

Penarikan kesimpulan dilakukan dengan menggunakan metode deduktif, yaitu menarik kesimpulan dari hal-hal yang bersifat umum ke dalam hal-hal yang bersifat khusus. Dalam hal ini, penulis mengkaji ketentuan hukum yang berlaku secara umum, kemudian mengaitkannya dengan kasus penyalahgunaan teknologi deepfake untuk memperoleh kesimpulan yang komprehensif dan sistematis.

PEMBAHASAN

A. Penyalahgunaan Teknologi Deepfake di Dunia Maya.

Perkembangan teknologi deepfake telah membuka peluang baru dalam pemanfaatan kecerdasan buatan, namun di sisi lain juga menimbulkan berbagai bentuk penyalahgunaan yang berdampak luas terhadap individu maupun masyarakat. Deepfake yang mampu menghasilkan konten audio dan visual yang sangat realistis menjadikannya sebagai alat yang efektif untuk melakukan manipulasi informasi. Dalam praktiknya, penyalahgunaan teknologi ini dapat diklasifikasikan ke dalam beberapa bentuk utama.

Pertama, penipuan digital (digital fraud). Dalam konteks ini, pelaku memanfaatkan teknologi deepfake untuk meniru wajah atau suara seseorang yang memiliki otoritas atau kepercayaan tinggi, seperti pimpinan perusahaan atau pejabat publik. Modus ini sering digunakan untuk mengelabui korban agar melakukan transfer dana atau memberikan informasi penting. Tingkat keberhasilan penipuan ini relatif tinggi karena korban sulit membedakan antara konten asli dan hasil manipulasi.

Kedua, iklan palsu (fraudulent advertising). Deepfake digunakan untuk mencatut identitas tokoh publik tanpa izin guna meningkatkan kredibilitas suatu produk. Dalam praktiknya, pelaku membuat video seolah-olah tokoh tersebut memberikan testimoni terhadap suatu produk, padahal kenyataannya tidak demikian. Hal ini merupakan bentuk penyesatan informasi yang merugikan konsumen serta melanggar hak individu yang identitasnya disalahgunakan.

Ketiga, pencurian identitas (identity theft). Teknologi deepfake memungkinkan penggunaan data biometrik seperti wajah dan suara seseorang tanpa persetujuan. Hal ini tidak hanya melanggar privasi, tetapi juga berpotensi digunakan untuk berbagai tindak kejahatan lainnya, seperti pembobolan sistem keamanan berbasis biometrik.

Keempat, disinformasi dan hoaks (misinformation and disinformation). Deepfake dapat digunakan untuk memproduksi konten palsu yang bertujuan mempengaruhi opini publik. Dalam konteks politik, misalnya, deepfake dapat digunakan untuk menyebarkan informasi yang menyesatkan guna menjatuhkan reputasi seseorang atau kelompok tertentu. Dampaknya tidak hanya bersifat individual, tetapi juga dapat mengganggu stabilitas sosial dan demokrasi.

B. Analisis Kasus Deepfake dalam Periklanan.

Fenomena penggunaan deepfake dalam periklanan digital menunjukkan adanya pelanggaran hukum yang cukup serius. Beberapa kasus yang beredar di media sosial memperlihatkan penggunaan wajah dan suara tokoh publik seperti dokter, pejabat negara, maupun selebritas untuk mempromosikan produk tertentu tanpa izin.

Dari perspektif hukum, terdapat beberapa pelanggaran yang dapat diidentifikasi. Pertama, tidak adanya izin penggunaan identitas, yang berarti pelaku telah melanggar hak privasi dan hak atas data pribadi individu. Kedua, informasi yang disampaikan bersifat menyesatkan, sehingga berpotensi merugikan konsumen yang mempercayai konten tersebut. Ketiga, pelanggaran etika bisnis, karena pelaku tidak menjalankan prinsip kejujuran dan transparansi dalam kegiatan periklanan.

Dampak dari praktik ini sangat luas. Bagi konsumen, hal ini dapat menimbulkan kerugian finansial akibat membeli produk yang tidak sesuai dengan klaim yang disampaikan. Bagi individu yang identitasnya disalahgunakan, hal ini dapat merusak reputasi dan kredibilitas. Sementara itu, secara umum, praktik ini dapat menurunkan tingkat kepercayaan masyarakat terhadap informasi digital yang beredar di internet.

C. Pengaturan Hukum di Indonesia.

Dalam konteks hukum di Indonesia, penyalahgunaan deepfake belum diatur secara khusus dalam satu regulasi tersendiri. Namun demikian, terdapat beberapa peraturan perundang-undangan yang dapat digunakan sebagai dasar hukum dalam menindak pelanggaran yang berkaitan dengan deepfake.

Pertama, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur mengenai penyebaran informasi bohong (hoaks) serta pencemaran nama baik melalui media elektronik. Ketentuan ini dapat diterapkan dalam kasus deepfake yang mengandung unsur penipuan atau merusak reputasi seseorang.

Kedua, Undang-Undang Perlindungan Konsumen, yang memberikan perlindungan kepada konsumen dari praktik bisnis yang tidak jujur, termasuk penyampaian informasi yang menyesatkan dalam periklanan.

Ketiga, Undang-Undang Perlindungan Data Pribadi (UU PDP), yang mengatur penggunaan data pribadi, termasuk data biometrik seperti wajah dan suara. Penggunaan data tersebut tanpa persetujuan merupakan pelanggaran hukum.

Keempat, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, yang mengatur kewajiban pelaku usaha untuk memberikan informasi yang benar, jelas, dan jujur dalam transaksi elektronik, termasuk dalam kegiatan periklanan digital.

D. Kelemahan Regulasi

Meskipun Indonesia telah memiliki sejumlah peraturan perundang-undangan yang dapat digunakan untuk menjerat pelaku penyalahgunaan teknologi digital, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Konsumen, serta Undang-Undang Perlindungan Data Pribadi (UU PDP), namun pengaturan hukum terkait teknologi deepfake masih menunjukkan berbagai kelemahan yang signifikan. Salah satu kelemahan utama adalah belum adanya regulasi yang secara spesifik dan komprehensif mengatur mengenai deepfake. Akibatnya, penanganan kasus yang berkaitan dengan deepfake masih bersifat sektoral dan parsial, serta sangat bergantung pada penafsiran aparat penegak hukum terhadap norma yang sudah ada.

Kondisi ini menimbulkan ketidakpastian hukum (legal uncertainty), terutama dalam menentukan unsur-unsur tindak pidana yang relevan. Misalnya, tidak semua bentuk manipulasi deepfake dapat secara langsung dikualifikasikan sebagai pencemaran nama baik atau penyebaran informasi bohong sebagaimana diatur dalam UU ITE. Selain itu, belum adanya definisi yuridis mengenai deepfake dalam sistem hukum Indonesia menyebabkan kesulitan dalam mengklasifikasikan perbuatan tersebut sebagai pelanggaran hukum tertentu.

Di samping itu, penegakan hukum yang belum optimal juga menjadi kendala serius. Kejahatan berbasis deepfake seringkali bersifat lintas negara (transnasional), sehingga membutuhkan kerja sama internasional yang efektif. Namun, keterbatasan yurisdiksi dan perbedaan sistem hukum antarnegara seringkali menghambat proses penegakan hukum. Selain itu, kapasitas aparat penegak hukum dalam memahami dan menangani kasus berbasis teknologi canggih masih perlu ditingkatkan.

Kelemahan lainnya terletak pada aspek pembuktian hukum. Dalam perkara yang melibatkan deepfake, pembuktian keaslian suatu konten digital menjadi sangat kompleks. Teknologi deepfake yang semakin canggih membuat konten hasil manipulasi sulit dibedakan dari konten asli, bahkan oleh ahli sekalipun. Hal ini menimbulkan tantangan dalam proses pembuktian di pengadilan, khususnya dalam memenuhi standar pembuktian yang sah menurut hukum acara.

E. Tantangan Hukum

Dalam menghadapi perkembangan teknologi deepfake, terdapat sejumlah tantangan hukum yang bersifat multidimensional. Pertama, perkembangan teknologi yang sangat cepat tidak sebanding dengan kecepatan pembentukan regulasi. Hukum sebagai instrumen sosial cenderung bersifat reaktif, sementara teknologi berkembang secara eksponensial. Akibatnya, hukum seringkali tertinggal dalam mengantisipasi dampak negatif dari inovasi teknologi.

Kedua, anonimitas pelaku di dunia maya menjadi hambatan utama dalam proses penegakan hukum. Pelaku kejahatan berbasis deepfake dapat dengan mudah menyembunyikan identitasnya melalui berbagai teknologi, seperti Virtual Private Network (VPN) dan platform anonim lainnya. Hal ini menyulitkan aparat penegak hukum dalam melakukan pelacakan dan identifikasi pelaku.

Ketiga, rendahnya literasi digital masyarakat juga menjadi tantangan yang tidak kalah penting. Banyak masyarakat yang belum memiliki kemampuan untuk membedakan antara konten asli dan konten hasil manipulasi deepfake. Kondisi ini menyebabkan masyarakat rentan menjadi korban penipuan, disinformasi, maupun propaganda yang disebarkan melalui media digital.

Keempat, kompleksitas pembuktian hukum dalam kasus deepfake menjadi tantangan tersendiri dalam sistem peradilan. Hakim dan aparat penegak hukum dituntut untuk memahami aspek teknis dari teknologi digital, termasuk metode verifikasi keaslian konten. Tanpa dukungan ahli digital forensik dan teknologi yang memadai, proses pembuktian akan menjadi sangat sulit dan berpotensi menimbulkan kesalahan dalam pengambilan putusan.

Kelima, tantangan juga muncul dari aspek etika dan perlindungan hak asasi manusia, terutama terkait dengan hak atas privasi, perlindungan data pribadi, dan kebebasan berekspresi. Pengaturan yang terlalu ketat berpotensi membatasi kebebasan berekspresi, sementara pengaturan yang terlalu longgar dapat membuka ruang bagi penyalahgunaan teknologi.

F. Upaya Penanggulangan

Menghadapi berbagai kelemahan regulasi dan tantangan hukum tersebut, diperlukan upaya penanggulangan yang bersifat komprehensif, sistematis, dan berkelanjutan. Upaya ini tidak hanya berfokus pada aspek penegakan hukum (represif), tetapi juga mencakup langkah-langkah pencegahan (preventif) dan penguatan kapasitas (capacity building).

Pertama, pembentukan regulasi khusus mengenai deepfake menjadi langkah yang sangat mendesak. Regulasi ini perlu memuat definisi yang jelas mengenai deepfake, ruang lingkup penggunaannya, serta sanksi hukum terhadap penyalahgunaannya. Selain itu, regulasi juga perlu mengatur mekanisme perlindungan bagi korban, termasuk hak untuk mendapatkan pemulihan (remedy).

Kedua, penguatan peran lembaga siber seperti Badan Siber dan Sandi Negara (BSSN) sangat diperlukan dalam menghadapi ancaman kejahatan berbasis deepfake. BSSN dapat berperan dalam melakukan deteksi dini, pemantauan, serta mitigasi terhadap penyebaran konten deepfake yang berpotensi merugikan masyarakat. Selain itu, peningkatan kapasitas sumber daya manusia di bidang keamanan siber juga menjadi hal yang krusial.

Ketiga, peningkatan literasi digital masyarakat merupakan langkah preventif yang sangat penting. Pemerintah bersama dengan lembaga pendidikan dan sektor swasta perlu melakukan edukasi kepada masyarakat mengenai bahaya deepfake serta cara mengenali konten manipulatif. Literasi digital yang baik akan membantu masyarakat menjadi lebih kritis dan tidak mudah terpengaruh oleh informasi yang menyesatkan.

Keempat, pengembangan dan pemanfaatan teknologi deteksi deepfake harus terus didorong. Pemerintah dapat bekerja sama dengan akademisi dan industri teknologi untuk mengembangkan sistem deteksi yang mampu mengidentifikasi konten deepfake secara akurat. Teknologi ini juga dapat digunakan sebagai alat bantu dalam proses penegakan hukum.

Kelima, penguatan kerja sama internasional juga menjadi faktor penting, mengingat kejahatan deepfake seringkali bersifat lintas batas negara. Kerja sama ini dapat dilakukan dalam bentuk pertukaran informasi, harmonisasi regulasi, serta bantuan hukum timbal balik (mutual legal assistance).

Dengan demikian, penanganan penyalahgunaan teknologi deepfake memerlukan pendekatan yang holistik dan kolaboratif, yang melibatkan pemerintah, aparat penegak hukum, akademisi, sektor swasta, serta masyarakat. Pendekatan ini diharapkan mampu menciptakan sistem hukum yang adaptif terhadap perkembangan teknologi sekaligus memberikan perlindungan yang optimal bagi masyarakat.

SIMPULAN

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa penyalahgunaan teknologi deepfake di dunia maya telah berkembang dalam berbagai bentuk, seperti penipuan digital, iklan palsu, pencurian identitas, serta penyebaran disinformasi. Teknologi ini memiliki kemampuan untuk memanipulasi konten audio dan visual secara sangat realistis, sehingga berpotensi besar menimbulkan kerugian bagi individu, konsumen, maupun masyarakat luas, serta mengancam kepercayaan publik terhadap informasi digital.

Dari perspektif hukum, Indonesia sebenarnya telah memiliki sejumlah regulasi yang dapat digunakan untuk menjerat pelaku penyalahgunaan deepfake, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Konsumen, dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Namun demikian, regulasi tersebut belum secara khusus dan komprehensif mengatur mengenai deepfake, sehingga masih terdapat kekosongan hukum (legal gap) dan ketidakpastian dalam penerapannya. Kondisi ini diperparah oleh berbagai kendala, seperti lemahnya penegakan hukum, kesulitan pembuktian digital, serta sifat kejahatan yang lintas negara dan anonim.

Selain itu, terdapat berbagai tantangan yang dihadapi dalam penanganan deepfake, antara lain perkembangan teknologi yang sangat cepat, rendahnya literasi digital masyarakat, serta kompleksitas dalam proses pembuktian hukum. Tantangan tersebut menunjukkan bahwa pendekatan hukum konvensional belum sepenuhnya mampu mengimbangi dinamika perkembangan teknologi digital.

Oleh karena itu, diperlukan langkah strategis yang komprehensif, meliputi pembentukan regulasi khusus terkait deepfake, penguatan kapasitas dan peran lembaga siber, peningkatan literasi digital masyarakat, serta pengembangan teknologi deteksi deepfake. Dengan pendekatan yang terintegrasi antara aspek hukum, teknologi, dan edukasi, diharapkan penanganan penyalahgunaan deepfake di Indonesia dapat dilakukan secara lebih efektif serta mampu memberikan perlindungan hukum yang optimal bagi masyarakat.

SARAN

Berdasarkan hasil penelitian dan simpulan yang telah diuraikan, terdapat beberapa saran yang dapat diajukan sebagai upaya dalam mengatasi penyalahgunaan teknologi deepfake di Indonesia.

1. Pemerintah perlu segera menyusun regulasi khusus yang mengatur teknologi deepfake secara komprehensif. Regulasi ini harus mencakup definisi hukum mengenai deepfake, batasan penggunaannya, mekanisme pertanggungjawaban hukum, serta sanksi yang tegas bagi pelaku penyalahgunaan. Dengan adanya aturan yang jelas, diharapkan dapat memberikan kepastian hukum serta memperkuat perlindungan terhadap masyarakat.

2. Penguatan kapasitas dan koordinasi antar lembaga penegak hukum dan lembaga siber perlu ditingkatkan. Lembaga seperti Badan Siber dan Sandi Negara (BSSN), Kepolisian, serta instansi terkait lainnya harus memiliki kemampuan teknis dan sumber daya manusia yang memadai dalam mendeteksi, menganalisis, dan menangani kasus berbasis teknologi deepfake. Selain itu, diperlukan peningkatan kerja sama lintas sektor dan lintas negara mengingat sifat kejahatan siber yang transnasional.

3. Peningkatan literasi digital masyarakat menjadi langkah preventif yang sangat penting. Pemerintah, lembaga pendidikan, dan sektor swasta perlu secara aktif melakukan edukasi kepada masyarakat mengenai bahaya deepfake, cara mengenali konten manipulatif, serta pentingnya verifikasi informasi sebelum menyebarkannya. Literasi digital yang baik akan membantu masyarakat menjadi lebih kritis dan tidak mudah terpengaruh oleh informasi yang menyesatkan.

4. Pengembangan dan pemanfaatan teknologi deteksi deepfake perlu terus didorong. Pemerintah dapat bekerja sama dengan perguruan tinggi, lembaga penelitian, dan perusahaan teknologi untuk menciptakan sistem deteksi yang akurat dan mudah diakses. Teknologi ini tidak hanya bermanfaat dalam penegakan hukum, tetapi juga dalam menjaga ekosistem informasi digital yang sehat.

5. Pelaku usaha di bidang digital dan periklanan diharapkan untuk menerapkan prinsip etika bisnis dan transparansi dalam penggunaan teknologi, termasuk tidak menggunakan teknologi deepfake tanpa izin atau untuk tujuan yang menyesatkan. Pengawasan terhadap platform digital juga perlu diperkuat untuk mencegah penyebaran konten yang melanggar hukum.

Dengan adanya langkah-langkah tersebut, diharapkan penanganan penyalahgunaan teknologi deepfake dapat dilakukan secara lebih efektif dan komprehensif, sehingga mampu memberikan perlindungan hukum yang optimal serta menjaga kepercayaan masyarakat terhadap informasi digital.

DAFTAR PUSTAKA

A. Peraturan Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

B. Buku

Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

McQuail, D. (2010). *McQuail's Mass Communication Theory* (6th ed.). Sage Publications.

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.

Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.

C. Jurnal, Artikel Ilmiah, dan Sumber Lain

Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs, 98*(1), 147–155.

Dwivedi, Y. K., Hughes, D. L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., … Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons, 63*(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

Mustak, M., Salminen, J., Mäntymäki, M., & Rahman, A. (2023). Deepfakes: Deceptions, mitigation, and opportunities. *Journal of Business Research, 154*, 113368. https://doi.org/10.1016/j.jbusres.2022.113368

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 39–52.

D. Jurnal dan Literatur Nasional

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Laporan Literasi Digital Nasional*. Jakarta: Kominfo.

Badan Siber dan Sandi Negara. (2022). *Laporan Tahunan Keamanan Siber Indonesia*. Jakarta: BSSN.

Sari, D. P., & Nugroho, A. (2021). Perlindungan hukum terhadap penyalahgunaan data pribadi di era digital. *Jurnal Hukum dan Pembangunan, 51*(2), 345–360.

Pratama, R. A. (2022). Tinjauan yuridis terhadap penyebaran hoaks dalam perspektif Undang-Undang ITE. *Jurnal Ilmu Hukum, 18*(1), 75–89.

E. Sumber Internet

European Commission. (2022). Tackling deepfakes and disinformation. Diakses dari https://ec.europa.eu

UNESCO. (2023). Artificial Intelligence and disinformation. Diakses dari https://www.unesco.org