RECHTSWETENSCHAP
Jurnal Mahasiswa Hukum

LEGAL LIABILITY FOR USING ARTIFICIAL INTELLIGENCE TO PRODUCE DEEPFAKES UNDER PERSONAL DATA PROTECTION LAW
PERTANGGUNGJAWABAN HUKUM ATAS PENGGUNAAN *ARTIFICIAL INTELLIGENCE* UNTUK *DEEPFAKE* MENURUT UU PERLINDUNGAN DATA PRIBADI

Kartika Ardina Raesyah Putri[1], Haris Djoko Saputro[2], Aliesa Amanita[3][1]
Prodi Ilmu Hukum Unjani
[2] Universitas Jenderal Achmad Yani

Article Info

Corresponding Author:
Penulis Korespondensi
kartikaardina9@gmail.com

History:
Submitted: xx-xx-xxxx
Revised: xx-xx-xxxx
Accepted: xx-xx-xxxx

Keyword:
Artificial Intelligence, Deepfake, Personal Data Protection, Strict Liability, Legal Responsibility.

Kata Kunci:
Artificial Intelligence, Deepfake, Perlindungan Data Pribadi, Strict Liability, Tanggung Jawab Hukum.

Copyright © 2025 by Jurnal Rechswetenschap

All writings published in this journal are personal views of the authors and do not

Abstract

The development of Artificial Intelligence (AI) technology has had a significant impact on various aspects of life, including the creation of deepfake content synthetic media capable of realistically mimicking an individual's identity. This phenomenon raises serious concerns regarding personal data protection and individual privacy rights, particularly in Indonesia, which currently lacks specific regulations governing AI. This study aims to examine the legal responsibilities surrounding the use of AI in creating deepfakes based on Law Number 27 of 2022 on Personal Data Protection (PDP Law), and to analyze the application of the strict liability principle to parties responsible for resulting damages. The research method used is normative juridical with a literature study approach. Data were obtained from laws and regulations, legal doctrines, and relevant academic literature, and were then analyzed qualitatively. The findings indicate that although the PDP Law provides a legal basis for personal data protection, a legal vacuum remains concerning liability for the use of AI to produce deepfakes. The main challenge lies in identifying the perpetrators and proving fault in autonomous AI systems. This study concludes that the principle of strict liability should be applied so that AI developers or users can be held accountable without the need to prove fault. Additionally, more specific regulations and stronger legal enforcement mechanisms are needed to protect society from the misuse of AI technology in the digital age.

Abstrak

Perkembangan teknologi *Artificial Intelligence* (AI) telah memberikan dampak yang signifikan dalam berbagai aspek kehidupan, termasuk dalam penciptaan konten *deepfake* media sintetis yang dapat meniru identitas seseorang secara realistis. Fenomena ini menimbulkan kekhawatiran serius terhadap perlindungan data pribadi dan hak privasi individu, terutama di

represent the views of the Constitutional Court.

Indonesia yang belum memiliki regulasi khusus mengenai AI. Penelitian ini bertujuan untuk mengkaji tanggung jawab hukum atas penggunaan AI dalam menciptakan *deepfake* berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribasi (UU PDP), serta menganalisis penerapan asas *strict liability* terhadap pihak-pihak yang bertanggung jawab atas kerugian yang ditimbulkan. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan studi kepustakaan. Data diperoleh dari peraturan perundang-undangan, doktrin hukum, dan literatur akademik yang relevan, kemudian dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa UU PDP telah memberikan dasar hukum perlindungan data pribadi, namun masih terdapat kekosongan hukum terkait tanggung jawab atas penggunaan teknologi AI dalam menghasilkan *deepfake*. Kesulitan utama terletak pada identifikasi pelaku dan pembuktian unsur kesalahan dalam sistem AI yang otonom. Penelitian ini menyimpulkan bahwa asas *strict liability* perlu diterapkan agar pelaku atau pengembang AI dapat dimintai pertanggungjawaban tanpa harus membuktikan unsur kesalahan. Selain itu, diperlukan regulasi tambahan yang lebih spesifik dan mekanisme penegakan hukum yang lebih kuat guna melindungi masyarakat dari penyalahgunaan teknologi AI di era digital.

A. PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi dari masa ke masa mencerminkan pada evolusi pemikiran dan inovasi manusia yang bertujuan untuk memenuhi kebutuhan hidup yang semakin kompleks. Pada masa prasejarah, teknologi diawali dengan adanya penemuan alat-alat sederhana seperti kapak batu dan tombak, yang digunakan untuk berburu dan bertahan hidup. Dalam memasuki era agraris, teknologi berkembang dengan ditemukannya alat-alat pertanian seperti cangkul dan bajak, yang telah mengingatkan efisiensi produksi pangan. Revolusi industri pada abad ke-18 menjadi titik balik signifikan dengan hadirnya mesin uap, yang mempercepat pada proses produksi dan memicu industrialisasi besar-besaran di seluruh dunia.[1]

Pada saat ini, kita telah berada dalam sebuah zaman yang sangat erat dengan teknologi komunikasi dan informasi. Kemajuan mengenai teknologi telah memberikan sumber informasi dan komunikasi yang sangat luas dari apa yang

[1] Lalu Adi Adha, "Digitalisasi Industri Dan Pengaruhnya Terhadap Ketenagakerjaan Dan Hubungan Kerja Di Indonesia," *Journal Kompilasi Hukum* 5, no. 2 (2020): 267–98, https://doi.org/10.29303/jkh.v5i2.49.

telah dimiliki oleh manusia. Revolusi informasi, biasanya dipahami sebagai perubahan yang telah dihasilkan oleh teknologi informasi. Sejarah perkembangan teknologi informasi pada hakekatnya ditentukan oleh penemuan alat untuk menyampaikan atau pertukaran informasi. Apabila dikaitkan dengan transformasi masyarakat yang diakibatkannya, dapat dikatakan perkembangan teknologi informasi dimulai sejak penemuan berbagai media tersebut yang tahapannya dari kertas, telepon, radio, televisi, hingga komputer. Penemuan tersebut dalam kurung waktu perkembangannya membawa akibat transformasi masyarakat dalam bentuk berbagai pola aktivitasnya.

Perkembangan teknologi telah membuat mata dunia semakin terbuka, segala informasi dalam saat ini sangat mudah diakses. Terlebih data pribadi saat ini sangat cepat untuk disebarluaskan dan diakses dengan mudah oleh siapapun tanpa adanya jaminan perlindungan yang memadai, maka sangat diperlukan peran hukum untuk mengatur dan juga mengelola teknologi. Dalam hal ini perlindungan data pribadi dan penyebaran informasi pribadi diatur dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.[2]

Perkembangan kecerdasan buatan AI telah menjadi salah satu pencapaian teknologi yang paling signifikan dalam beberapa tahun terakhir. AI adalah kecerdasan yang ditambahkan kepada suatu sistem yang bisa diatur dalam konteks ilmiah atau bisa disebut *Artificial Intellegence* atau hanya disingkat AI, didefinisikan sebagai kecerdasan entitas ilmiah.[3] Sejarah (AI) dimulai pada tahun 1956, Ketika John McCarthy dan sekelompok ilmuwan komputer lainnya mengadakan konferensi di Dartmouth College, yang dikenal sebagai tonggak kelahiran AI.[4] Konferensi ini bertujuan untuk menyatukan para peneliti dari berbagai bidang untuk mengekplorasi potensi mesin yang dapat meniru kecerdasan manusia.

---

[2] "Undang-Undang Nomor 27 Tahun 2022." JDIH Kominfo, Kementerian Komunikasi dan Informatika Republik Indonesia, 2022, jdih.kominfo.go.id/produk_hukum/view/id/832/t/undangundang+nomor+27+tahun+2022. diakses 4 Dec. 2024.

[3] Joseph Teguh Santoso, Kecerdasan Buatan (Artificial Intelligence, 2023).

[4] "Mengenal Sejarah AI & Perkembangannya." *BNCC Student Activity BINUS*, 23 Aug. 2024, student-activity.binus.ac.id/bncc/2024/08/23/mengenal-sejarah-ai-perkembangannya/.

Kebangkitan AI Kembali pada tahun 1980-an dengan pengenalan sistem pakar yang mampu meniru keputusan seorang ahli dalam bidang tertentu. Pada periode ini, teknologi komputer mulai berkembang pesat, yang dapat memungkinkan algoritma lebih kompleks untuk diterapkan dalam berbagai aplikasi. Meskipun demikian, penelitian terus berlanjut, dan pada tahun 1997, momen bersejarah terjadi ketika komputer *Deep Blue* dari IBM berhasil mengalahkan juara dunia catur Garry Kasparov, menandai kemampuan AI untuk bersaing dengan manusia dalam permainan strategi yang kompleks.[5]

Memasuki abad ke-21, perkembangan AI semakin pesat berkat kemajuan dalam komputasi dan ketersediaan data besar[6]. Teknologi *machine learning* dan *deep learning* menjadi fokus utama penelitian AI, memungkinkan komputer untuk belajar dari data dan meningkatkan kinerjanya seiring waktu. *Machine learning* adalah cabang dari kecerdasan buatan AI dan ilmu computer yang berfokus pada penggunaan data dan algoritma untuk meniru cara manusia belajar, secara bertahap meningkatkan akurasinya.[7] *Deep learning* adalah cabang dari *machine learning* yang terinpirasi oleh struktur dan fungsi otak manusia, yang disebut sebagai jaringan saraf tiruan atau *artificial neural network*.[8] Penerapan AI kini merambah berbagai sektor, termasuk kesehatan, transportasi, perbankan, dan hiburan. Asisten virtual seperti Siri dan Alexa serta algoritma rekomendasi di *platform streaming* menjadi contoh nyata bagaimana AI telah terintegrasi dalam kehidupan sehari-hari.

Saat ini, kecerdasan buatan tidak hanya menjadi alat bantu tetapi juga bagian integral dari inovasi di berbagai industri. Dengan kemajuan teknologi yang terus berlanjut, masa depan AI menjanjikan potensi yang lebih besar untuk mempermudah kehidupan manusia. Dalam beberapa tahun ke depan, kita dapat mengharapkan perkembangan lebih lanjut dalam kemampuan AI yang akan

---

[5] "Perkembangan AI dari Masa ke Masa: Dari Konsep hingga Teknologi Modern." *Harian Sriwijaya*, hariansriwijaya.com/perkembangan-ai-dari-masa-ke-masa-dari-konsep-hingga-teknologi-modern/.

[6] Mursalin, Firdaus, Azwa Fazilatunnisa, Ratna Dwi Puspita, Muhammad Riza Rahmatullah, dan Ann Anshori, "Revolusi Teknologi: Tantangan Masa Depan Integrasi Teknologi Kecerdasan Buatan (AI) dalam Arsitektur Komputer."

[7] Emi Sita Eriana and Afrizal Zein, *Artificial Intelligence (AI)* (2023).

[8] Ibid.

membuka peluang baru di bidang penelitian, bisnis, dan masyarakat secara keseluruhan.

Penyalahgunaan kecerdasan buatan AI telah menjadi isu yang kompleks dan memunculkan tantangan besar dalam penegakan hukum pidana, terutama dalam ranah kejahatan dunia maya atau *cybercrime*. *Cybercrime* pada dasarnya adalah perbuatan jahat yang dilakukan melalui dunia maya dengan menggunakan internet atau komputer atau peralatan lainnya, dimana tindakan tersebut dapat dikatakan suatu kejahatan. Dalam hal ini internet sebagai media yang digunakan untuk penyebaran pornografi, maka kebijakan utama yang harus diambil adalah pengaturan internet itu sendiri.[9] AI, yang awalnya dirancang untuk meningkatkan efisiensi dan inovasi, kini sering disalahgunakan untuk aktivitas ilegal, seperti manipulasi data pribadi, penyebaran konten *deepfake,* hingga serangan *cyber.* Kejahatan ini tidak hanya menimbulkan kerugian material, tetapi juga merusak privasi dan keamanan masyarakat. Oleh karena itu, regulasi yang adaptif sangat diperlukan untuk mengatasi berbagai tantangan yang muncul seiring kemajuan teknologi digital.

AI telah berkembang pesat dalam beberapa tahun terakhir, dan salah satu dari dampak negatif yang muncul adalah kemampuan untuk menciptakan *deepfake* atau konten media yang dimanipulasi menggunakan teknologi AI untuk menyamarkan identitas atau ucapan seseorang. *Deepfake* memanfaatkan algoritma pembelajaran mendalam untuk mengubah gambar, video, atau suara, sehingga dapat membuat individu tampak melakukan atau mengatakan sesuatu yang sebenarnya tidak pernah terjadi. Penggunaan *deepfake* ini menimbulkan potensi besar bagi penyebaran disinformasi, manipulasi opini publik, serta pelanggaran terhadap privasi dan reputasi seseorang.

Perkembangan hukum dalam konteks kecerdasan buatan AI telah menjadi isu penting seiring pesatnya kemajuan teknologi dari berbagai sektor. AI sangat membawa dampak yang signifikan, mulai dari efisiensi operasional hingga perubahan pola interaksi manusia dengan teknologi. Namun pada kemajuan ini dapat memunculkan hukum baru, termasuk privasi data, tanggung

[9] Emi Sita Eriana and Afrizal Zein, Artificial Intelligence (AI) (2023).

jawab hukum, dan juga dampak sosial dari penggunaan AI. Di berbagai negara seperti Uni Eropa, regulasi seperti *General Data Protection Regulation* (GDPR) telah diimplementasikan untuk menangani dampak AI terhadap perlindungan data pribadi. *General Data Protection Regulation* (GDPR) adalah regulasi yang telah diterapkan oleh Uni Eropa untuk melindungi data pribadi individu dan mengatur cara data tersebut dikumpulkan, diproses, dan disimpian oleh organisasi. *General Data Protection Regulation* (GDPR) telah diberlakukan pada 25 Mei 2018, dengan tujuan utama untuk memperkuat dan menyelaraskan perlindungan data pribadi bagi warga Uni Eropa serta memberikan kontrol yang lebih besar kepada individu. Di sisi lain, Amerika Serikat telah mengatur penggunaan AI dalam aspek tertentu, termasuk penipuan berbasis teknologi dan privasi digital.

Secara keseluruhan, *General Data Protection Regulation* (GDPR) bukan hanya sekedar regulasi tentang perlindungan data pribadi, tetapi juga merupakan langkah penting menuju perlindungan privasi di era digital. Meskipun *General Data Protection Regulation* (GDPR) tidak secara khusus membahas masalah *cybersecurity* dalam konteks yang lebih luas, regulasi ini mengharuskan organisasi untuk mengamankan data pribadi terhadap ancaman *cyber* dan memastikan bahwa keamanan data menjadi bagian integral dari kebijakan pengolahan data mereka. Organisasi diwajibkan untuk mengimplementasikan langkah-langkah pengamanan yang sesuai dan melaporkan pelanggaran data dengan cepat untuk meminimalkan dampaknya terhadap individu. Oleh karena itu, prinsip-prinsip dan ketentuan dalam *General Data Protection Regulation* (GDPR) dapat dianggap sebagai dasar yang kuat untuk mengelola ancaman *cyber* yang terkait dengan perlindungan data pribadi. Dengan demikian dapat memberikan kontrol lebih besar kepada individu atas informasi pribadi mereka dan menetapkan standar tinggi bagi organisasi dalam pengelolaan data, *General Data Protection Regulation* (GDPR) berpotensi menjadi model bagi regulasi privasi di seluruh dunia.

Di Indonesia, pengaturan hukum terhadap AI masih dalam tahap awal, meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sudah memberikan dasar

hukum. Tantangan yang paling utama adalah bagaimana hukum dapat mengantisipasi dari risiko penyalahgunaan AI, seperti *deepfake* dan pengambilan keputusan otomatis yang tidak transparan. Selain itu, ada kebutuhan untuk menetapkan tanggung jawab hukum, baik pada pengembang, pengguna, maupun penyedia teknologi AI. Dengan demikian, pengembangan hukum yang adaptif dan kolaboratif menjadi kebutuhan mendesak agar AI dapat dimanfaatkan secara etis dan bertanggung jawab.

Penyalahgunaan kecerdasan buatan AI telah menjadi isu yang kompleks dan memunculkan tantangan besar dalam penegakan hukum pidana. AI yang awalnya telah dirancang untuk meningkatkan efisiensi dan inovasi di berbagai sektor, kini sangat sering disalahgunakan untuk aktivitas ilegal, seperti penyebaran konten *deepfake* dan serangan *cyber* yang canggih. Teknologi ini juga digunakan untuk pencurian identitas, manipulasi data, hingga penciptaan informasi palsu yang dapat merusak reputasi individu atau organisasi. Fenomena ini tidak hanya menimbulkan pada kerugian material tetapi juga berdampak pada pelanggaran hak privasi dan ancaman terhadap keamanan publik.

Dalam konteks kecerdasan buatan AI dan penyalahgunaan teknologi seperti *deepfake*, Asas *strict liability* adalah pertanggungjawaban pidana tanpa kesalahan, dimana pembuat sudah dapat dipidana apabila dia telah melakukan perbuatan pidana sebagaimana dirumuskan dalam Undang-Undang, tanpa melihat bagaimana sikap batinnya. Dalam kasus penggunaan *deepfake* untuk menyebarkan informasi palsu atau mencemarkan nama baik, pihak yang mengembangkan, menyediakan, atau menggunakan teknologi tersebut dapat dimintai pertanggungjawaban berdasarkan *strict liability* apabila teknologi tersebut terbukti menyebabkan kerugian.

Dalam perspektif hukum pidana, tantangan utama adalah mengidentifikasi pelaku yang berada di balik teknologi yang kompleks ini. Teknologi AI sering kali bekerja melalui sistem yang otonom, sehingga menimbulkan kesulitan dalam menentukan tanggung jawab pidana, baik terhadap pengembang, pengguna, atau pihak lain yang terlibat secara tidak langsung. Selain itu, regulasi yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi

(UU PDP), masih belum sepenuhnya mencakup bentuk-bentuk penyalahgunaan AI yang terus berkembang.

Pentingnya pengaturan hukum pidana yang spesifik terhadap penyalahgunaan AI menjadi sangat mendesak. Hal ini melibatkan penyesuaian mengenai elemen kesalahan pidana, penguatan sanksi terhadap penyelahgunaan teknologi, serta peningkatan kolaborasi internasional untuk menghadapi kasus-kasus yang bersifat lintas batas. Dengan pendekatan hukum yang adaptif dan progresif, penyalahgunaan AI dapat dicegah dan ditangani secara efektif, sehingga memberikan perlindungan yang lebih baik terhadap masyarakat di era digital ini.

Maka di Indonesia, fenomena ini telah menjadi perhatian serius karena dapat mengakibatkan ketidakpastian hukum dan merugikan kelompok tertentu. Kekosongan hukum dalam konteks penyalahgunaan kecerdasan buatan AI dapat dijadikan celah yang digunakan untuk penyalahgunaan teknologi AI, yang dapat merugikan individu dan masyarakat. Kekosongan hukum dalam penyalahgunaan AI juga menimbulkan tantangan etis yang kompleks. Misalnya, penggunaan AI dalam sistem pemantauan atau penegakan hukum dapat mengarah pada pelanggaran hak asasi manusia jika tidak ada regulasi yang jelas untuk melindungi individu dari penyalahgunaan.

Pada tingkat internasional, banyak negara juga menghadapi tantangan yang serupa dalam mengatur penggunaan AI. Meskipun Uni Eropa telah mengambil langkah maju dengan menetapkan regulasi yang lebih ketat terkait AI berdasarkan tingkat risiko, banyak negara lain yang masih mengkaji untuk menyusun kerangka hukum yang efektif. Seperti Australia juga masih mengembangkan pedoman dan standar untuk mengatur penggunaan AI, tetapi belum ada konsensus global mengenai bagaimana seharusnya teknologi ini diatur. Kekosongan hukum ini berpotensi menciptakan ketidakadilan dan risiko bagi masyarakat, terutama dalam konteks privasi dan keamanan data.

Oleh karena itu, penting untuk menciptakan regulasi yang tidak hanya mengatur penggunaan teknologi tetapi juga melindungi hak-hak individu. Sebagai langkah menuju solusi, diperlukan kolaborasi antara pemerintah, akademisi, dan sektor swasta untuk mengembangkan kerangka hukum yang

komprehensif terkait AI. Indonesia memiliki kesempatan untuk belajar dari pengalaman negara lain yang telah lebih dulu menerapkan regulasi terkait AI. Dengan membentuk lembaga khusus yang bertanggung jawab atas pengawasan dan penegakan hukum terkait AI, serta melibatkan berbagai pemangku kepentingan dalam proses pembuatan kebijakan, Indonesia dapat menciptakan regulasi yang responsif terhadap perkembangan teknologi sekaligus melindungi kepentingan masyarakat secara keseluruhan.

Menurut *Cambridge Dictionary*, *deepfake* adalah "rekaman video atau suara yang menggantikan wajah atau suara seseorang dengan wajah atau suara orang lain, sehingga tampak nyata."[10] Berdasarkan uraian tersebut *deepfake* dapat diartikan sebagai teknologi berbasis AI yang memungkinkan penggantian wajah atau suara seseorang dalam rekaman video atau audio dengan wajah atau suara orang lain secara realistis, sehingga terlihat autentik. Fenomena ini menciptakan tantangan signifikan, terutama dalam konteks hukum, karena *deepfake* sering digunakan untuk tujuan yang tidak etis, seperti penyebaran informasi palsu, pencemaran nama baik, atau bahkan pemerasan. *Deepfake* telah menjadi isu sensitif dalam beberapa tahun terakhir. Fenomena ini tidak hanya menimbulkan kerugian psikologis, sosial, dan ekonomi bagi korban tetapi juga menciptakan tantangan signifikan dalam menentukan pelaku tindak pidana.

Menentukan pelaku tindak pidana *deepfake* menjadi sangat sulit karena beberapa faktor. Pertama, teknologi AI yang digunakan dalam membuat *deepfake* sangat canggih dan sulit untuk diacak-acak. Kedua pelaku dapat menggunakan *platform-platform* daring yang anonim untuk melakukan aksinya, sehingga identitas mereka sulit ditemukan. Ketiga, konten *deepfake* sering kali difungsikan sebagai alat penipuan, sehingga sulit untuk membedakan mana yang legal dan ilegal.

Maka dalam hal ini penulis akan mengambil identifikasi masalah yaitu:

1. Bagaimana pengaturan hukum terkait penggunaan *Artificial Intelligence* (AI) menurut Undang-Undang Perlindungan Data Pribadi?

[10] "Edukasi Hukum: Tindakan Deepfake," Bullyid, https://bullyid.org/edukasi-hukum-tindakan-deepfake/.

2. Bagaimana penerapan asas *Strict Liability* dalam penggunaan *Artificial Intelligence* (AI) yang menciptakan konten *deepfake*?

B. HASIL DAN PEMBAHASAN

1. Pengaturan Hukum Terkait Penggunaan *Artificial Intelligence* Menurut Undang-Undang Perlindungan Data Pribadi

Perlindungan data pribadi merupakan hak asasi manusia yang dijamin dalam sistem hukum Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mendefinisikan data pribadi dalam Pasal 1 angka 1 sebagai:

> *"setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik."*

Dalam Undang-Undang Perlindungan Data Pribadi (UU PDP), khususnya pasal 32 dan pasal 33, ditegaskan adanya kewajiban yang melekat pada pengendali data pribadi dan prosesor data. Pengendali data adalah pihak yang menentukan tujuan dan kendali dari pemrosesan data, sedangkan prosesor data adalah pihak yang memproses data atas nama pengendali data. Dalam konteks AI, kewajiban ini menjadi sangat penting mengingat AI sering kali mengolah data pribadi dalam jumlah besar untuk kebutuhan analisis atau pembuatan konten baru seperti *deepfake*.

Pasal 32 UU PDP mengatur tentang kewajiban pengendali data, yang berbunyi:

> *"Pengendali Data Pribadi wajib memberikan akses kepada Subjek Data Pribadi terhadap Data Pribadi yang diproses beserta rekam jejak pemrosesan Data Pribadi sesuai dengan jangka waktu penyimpanan Data Pribadi."*

Sementara itu, pasal 33 UU PDP mengatur kewajibab Prosesor Data yang menyatakan:

> *"Pengendali Data Pribadi wajib menolak memberikan akses perubahan terhadap Data Fribadi kepada Subjek Data Pribadi dalam hal:*
>
> *a) membahayakan keamanan, kesehatan fisik, atau kesehatan mental Subjek Data Pribadi dan/ atau orang lain;*

b) *berdampak pada pengungkapan Data Pribadi milik orang lain; dan/ atau*
c) *bertentangan dengan kepentingan pertahanan dan keamanan nasional."*

Dengan adanya ketentuan ini dalam penerapan AI, baik pengembang maupun pengguna teknologi AI harus memastikan bahwa setiap pengolahan data pribadi dilakukan berdasarkan dasar hukum yang sah dan dengan persetujuan yang sah dari subjek data apabila diperlukan. Pengendali data wajib memastikan keamanan, akurasi, serta kerahasiaan data, sedangka prosesor data hanya boleh meproses data sesuai dengan instruksi dari pengendali data, tidak untuk kepentingan lain.

Di samping itu, aspek lain yang harus diperhatikan dalam penggunaan AI adalah perlindungan hak-hak subjek data pribadi. Dalam penggunaan AI, perlindungan terhadap hak-hak ini menjadi semakin krusial mengingat AI memiliki potensi untuk memproses data pribadi secara otomatis dalam jumlah besar, dan untuk berbagai tujuan. UU PDP secara tegas mengatur hak-hak subjek data dalam Pasal 5 sampai dengan Pasal 14, yang mencakup hak untuk memperoleh informasi, hak untuk menarik persetujuan, serta hak untuk mengajukan keberatan atas tindakan pemrosesan data.

Pasal 6 UU PDP

"Subjek Data Pribadi berhak melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi tentang dirinya sesuai dengan tujuan pemrosesan Data Pribadi."

Mengenai penggunaan AI, setiap individu berhak mengetahui apakah datanya digunakan untuk algoritma AI, atau bahkan untuk menghasilkan konten seperti *deepfake*. Selain itu, pasal 7 UU PDP menegaskan hak subjek data untuk memperbarui atau memperbaiki data pribadinya apabila terdapat ketidakakuratan, sehingga menghindari kesalahan dalam hasil kerja AI.

Dalam kerugian yang dialami pemilik subjek data dapat meminta tanggung jawab hukum dalam penggunaan AI yang melibatkan data pribadi. Data pribadi merupakan aspek yang sangat penting untuk memastikan bahwa pemanfaatan teknologi ini tidak merugikan individua tau pihak lain. hal ini menjadi semakin relevan apabila mengingat potensi penyalahgunaan AI, seperti pembuatan *deepfake*, yang dapat merusak reputasi seseorang, menyebarkan informasi palsu atau melanggar privasi

individu. UU PDP memberikan landasan hukum terkait tanggung jawab hukum yang perlu diberi oleh Pengendali data dan Prosesor data.

Pasal 47 UU PDP mengatur mengenai tanggung jawab pengendali data, yang berbunyi:

> *"pengendali data pribadi wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip perlindungan data pribadi."*

Pasal 47 mengatur bahwa apabila terjadi pelanggaran terkait perlindungan data pribadi, seperti penyalahgunaan data yang diolah sistem AI, pihak pengendali data dapat dikenakan sanksi administratif. Pasal 47 mengatur bahwa apabila terjadi pemrosesan data pribadi yang tidak sesuai dengan ketentuan undang-undang atau terjadi kebocoran data pribadi, pihak yang bertanggung jawab dapat dikenakan sanksi administratif berupa denda, teguran, atau bahkan penghentian proses pengolahan data tersebut.

Dalam penggunaan AI yang dapat menghasilkan *deepfake* , perlu diingat bahwa setiap individu yang terlibat dalam pembuatan atau penyebaran konten tersebut dapat dikenakan tanggung jawab pidana atas dasar pelanggaran hak privasi atau pencemaran nama baik. Hal ini semakin relevan dengan adanya pasal-pasal yang melindungi hak subjek data pribadi, seperti hak untuk menghapus data pribadi, hak untuk menarik persetujuan, dan hak untuk mengajukan keberatan jika data pribadi mereka digunakan untuk tujuan yang tidak sah.

UU PDP memberikan hak-hak penting bagi subjek data, seperti hak untuk mengakses, memperbaiki, dan menghapus data pribadi mereka, yang sangat relevan dalam menghadapi tantangan penggunaan AI yang dapat merugikan individu, seperti manipulasi wajah dan suara tanpa izin. UU ini juga mewajibkan pengendali data untuk melaksanakan langkah-langkah keamanan yang memadai guna melindungi data pribadi dari penyalahgunaan atau akses yang tidak sah, yang memberikan dasar hukum untuk menanggapi ancaman yang dihadirkan oleh teknologi AI.

Untuk mencegah terkait penyalahgunaan AI terhadap data pribadi, penguatan hukum di Indonesia perlu dilakukan dengan beberapa langkah strategis. Seperti regulasi yang lebih spesifik dan komprehensif mengenai penggunaan AI dalam pengolahan data pribadi harus segera disusun. Hal ini termasuk ke dalam penetapahan standar yang jelas mengenai bagaimana algoritma AI dapat digunakan dalam mengolah data pribadi, serta

aturan yang memastikan transparansi dan akuntabilitas dalam setiap pengguna teknologi AI. Selanjutnya, perlu adanya pembentukan Lembaga pengawas independen yang memiliki wewenang untuk mengawasi penggunaan teknologi AI, terutama yang berhubungan dengan manipulasi data pribadi, seperti dalam pembuatan *deepfake* .

Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam penanganan tindak pidana siber tidak dapat berdiri sendiri, melainkan harus memperhatikan keberadaan undang-undang lain yang relevan. Selain UU PDP, salah satu undang-undang yang sering terkait adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur transaksi elektronik dan tindak pidana terkait teknologi informasi, seperti pencemaran nama baik, penipuan, atau penyebaran konten ilegal. Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) tetap berlaku dalam menangani tindak pidana umum, seperti pencurian data atau penipuan melalui dunia maya. Oleh karena itu, sinergi antara berbagai undang-undang ini sangat penting untuk memastikan perlindungan data pribadi, memberikan keadilan bagi korban, serta mencapai penegakan hukum yang efektif dalam konteks dunia maya.

2. Penerapan Asas *Strict Liability* Dalam Penggunaan *Artificial Intelligence* Yang Mencipptakan Konten *Deepfake*

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*) yang digunakan untuk menciptakan konten *deepfake* telah menghadirkan tantangan hukum baru, khususnya dalam konteks pertanggungjawaban terhadap kerugian yang ditimbulkan. Salah satu pendekatan yang dianggap relevan dalam menjawab tantangan tersebut adalah penerapan asas *strict liability*, yaitu pertanggungjawaban hukum tanpa mensyaratkan pembuktian unsur kesalahan (*mens rea*) dari pelaku.

Menurut Barda Nawawi Arief, *strict liability* adalah konsep hukum pertanggungjawaban mutlak (tanpa kesalahan), yaitu bentuk kejahatan yang di dalamnya tidak mensyaratkan adanya unsur kesalahan dalam pemidanaan, tetapi hanya disyaratkan adanya suatu perbuatan. [11] *Strict liability* merupakan konsep pertanggungjawaban hukum yang tidak mensyaratkan adanya pembuktian unsur kesalahan untuk mempidanakan seseorang. Dalam penerapannya, pelaku dapat dimintai

[11] Barda Nawawi Arief, *Perbandingan Hukum Pidana* (Jakarta: Rajawali Pers, 2011).

pertanggungjawaban hanya karena telah melakukan perbuatan yang telah dilarang oleh hukum, tanpa perlu dibuktian apakah ada niat jahat atau kelalaian.

Asas *strict liability* merupakan prinsip pertanggungjawaban hukum tanpa perlu dibuktikan unsur kesalahan. Dalam konteks hukum perdata, asas ini banyak diterapkan dalam kasus-kasus yang berkaitan dengan tanggung jawab atas produk berbahaya, perlindungan konsumen, dan lingkungan hidup. Tujuan utama dari penerapan asas ini adalah untuk melindungi pihak yang rentan dari akibat yang merugikan, tanpa harus melalui pembuktian yang rumit terhadap unsur kesalahan dari pelaku. Hal ini bertujuan untuk mempercepat penegakan hukum di bidang tertentu yang sangat penting untuk kepentingan umum, seperti lingkungan hidup, Kesehatan masyarakat, dan teknologi informasi. Namun asas *strict liability* sebagai sistem pembuktian dalam peradilan pidana belum dikenal sehingga penggunaan *strict liability* saat ini hanya dalam sistem pembuktian peradilan perdata. Untuk diterapkannya asas ini perlu adanya reformasi dalam KUHP, KUHAP, dan undang-undang pidana khusus lainnya dengan suatu Batasan tertentu yang mengatur penggunaan asas ini.

Konsep *strict liability* atau pertanggungjawaban mutlak merupakan prinsip hukum yang menyatakan bahwa seseorang atau badan hukum dapat dimintai pertanggungjawaban atau suatu kerugian tanpa perlu dibuktian adanya unsur kesalahan. Dalam konteks hukum Indonesia, prinsip ini secara eksplisit diatur dan diterapkan dalam beberapa sektor hukum tertentu, khususnya dalam hukum perlindungan konsumen dan hukum lingkungan. Misalnya, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menetapkan bahwa pelaku usaha bertanggung jawab atas kerugian yang diderita konsumen akibat produk yang cacat atau berbahaya, meskipun tidak terbukti adanya kesalahan dari pihak pelaku usaha. Demikian pula dalam Undang-Undang Nomor 32 Tahun 2009 tentang Perlindungan dan Pengelolaan Lingkungan Hidup, pelaku usaha dapat dimintai pertanggungjawaban mutlak atas kerusakan lingkungan yang ditimbulkan akibat kegiatan usahanya.

Teori *strict liability* berkembang dari pandangan bahwa dalam kondisi tertentu, demi efektivitas perlindungan hukum, pertanggungjawaban harus dibebankan kepada pelaku tanpa melihat unsur subjektif. Menurut teori ini, perlindungan korban lebih diutamakan daripada mempertimbangkan motif atau niat pelaku hal ini sejalan dengan pendapat sudarto, yang menyatakan bahwa dalam keadaan tertentu hukum pidana

dapat mengesampingkan asas kesalahan untuk mencapai tujuan perlindungan hukum yang lebih luas.

Dalam kasus *deepfake* dapat dikatakan risiko besar terhadap privasi dan reputasi pribadi akibat teknologi *deepfake* menjadi salah satu perhatian utama dalam era perkembangan AI. *Deepfake* memungkinkan manipulasi gambar, suara, dan video seseorang sedemikian rupa hingga tampak autentik, namun, dalam kenyataannya adalah hasil rekayasa. Ketika data wajah, suara atau perilaku seseorang diambil tanpa izin dan dimanipulasi, ha katas privasi individu dapat dikatakan dilanggar secara serius. Informasi pribadi yang semestinya bersifat rahasia dapat tersebat luas di ruang publik, bahkan dalam bentuk yang mempermalukan atau merusak nama baik seseorang. Selain itu, reputasi pribadi juga sangat rentan hancur akibat konten *deepfake* , terutama apabila konten tersebut mengandung unsur pornografi, ujaran kebencian, penipuan, atau fitnah. Dampak sosial dari tersebarnya konten *deepfake* bisa sangat luas, termasuk hilangnya kepercayaan masyarakat, kerugian karier tekanan psikologis, dan bahkan stigma sosial jangka Panjang.

Di Indonesia, sistem hukum pidana masih menjunjung tinggi asas legalitas dan asas kesalahan sebagaimana tertuang dalam Pasal 1 ayat (1) KUHP. Namun, perkembangan *cybercrime*, termasuk penyebaran konten deepfake yang merusak reputasi dan data pribadi seseorang, menuntut adanya pendekatan yang lebih progresif dan adaptif. Hal ini disebabkan oleh kenyataan bahwa pelaku kejahatan digital sering kali bersifat anonim, tersembunyi di balik teknologi, serta sulit dijangkau oleh mekanisme hukum konvensional.

Dalam beberapa kasus untuk membuktikan unsur kesalahan mengenai pembuatan atau penyebaran konten *deepfake* merupakan tantangan besar dalam penegaran hukum. *deepfake* sebagai teknologi yang melibatkan manipulasi gambar, suara, dan video menggunakan kecerdasan AI sering kali menghasilkan konten yang sangat realistis, sehingga sulit dibedakan dari kenyataan. Hal ini mempersulit pihak berwenang dalam mengidentifikasi niat jahat atau kesalahan yang disengaja oleh pelaku.

Pembuatan dan penyebaran *deepfake* seringkali dilakukan secara anonim melalui internet, dan pelaku dapat dengan mudah menyembunyikan identitas mereka. Dalam kondisi seperti ini, membuktikan unsur kesalahan atau niat jahat pelaku menjadi sangat sulit, bahkan hampir mustahil, karena penggunaan teknologi yang memungkinkan

manipulasi gambar dan suara dengan sangat realistis. Oleh karena itu, penerapan *strict liability* memberi jalan untuk menegakkan hukum meskipun identitas atau niat pelaku sulit dibuktikan. Dengan tanggung jawab mutlak, pelaku yang terlibat dalam pembuatan atau penyebaran *deepfake* dapat dikenai sanksi tanpa perlu menunggu pembuktian niat buruk.

Penyebaran *deepfake* dapat melibatkan banyak pihak dan dilakukan dalam skala yang sangat besar melalui platform digital. Penggunaan *strict liability* dalam hal ini membantu penegak hukum untuk lebih cepat dan efisien dalam menanggulangi penyebaran konten palsu tanpa harus menghabiskan waktu untuk mencari bukti-bukti kesalahan atau kelalaian dari pelaku. Ini berfungsi untuk mencegah kerugian yang lebih luas, karena pelaku yang bertanggung jawab akan dikenai sanksi meskipun tidak ada bukti langsung yang menunjukkan niat jahat mereka.

Apabila dilihat dari asas *strict liability* mengenai *deepfake* dapat berfungsi untuk melindungi korban dari penyalahgunaan teknologi yang dapat menyebabkan kerusakan besar terhadap privasi dan reputasi. Dengan menganggap perbuatan pembuatan dan penyebaran *deepfake* sebagai perbuatan melawan hukum, tanpa perlu membuktikan unsur kesalahan atau niat jahat, hukum dapat dengan lebih efektif menangani permasalahan ini.

Mengenai sistem hukum di Indonesia menganggap konsep *strict liability* sebagai hal yang baru, sistem hukum ini bahkan hanya familiar pada negara eropa yang menganut sistem hukum Eropa Kontinental dengan pengecualian terhadap hal pelanggaran karena sejatinya konsep *strict liability* awalnya hanya terdapat pada *common law system*.[12]

Di tingkat global, prinsip *strict liability* telah mulai diterapkan dalam rancangan regulasi seperti *Artificial Intelligence Liability Directive* (AILD) oleh Uni Eropa, yang memberikan mekanisme tanggung jawab otomatis terhadap kerugian yang diakibatkan oleh sistem AI berisiko tinggi. Di Amerika Serikat, pendekatan hukum gugatan perdata terhadap konten deepfake berbasis tort law juga mulai berkembang untuk memberikan perlindungan terhadap korban.

---

[12] Ni Made Yordha Ayu Astiti, "*Strict Liability of Artificial Intelligence: Pertanggungjawaban kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban*," *Jurnal Magister Hukum Udayana* 12, no. 4 (2023): 963.

Di Uni Eropa, dikembangkan melalui *Artificial Intelligence Liability Directive (AILD)*, yang memperkenalkan prinsip *presumption of causality* untuk meringankan beban pembuktian korban dalam kasus kerugian akibat AI. Hal ini menunjukkan bahwa asas *strict liability* sangat efektif diterapkan dalam menghadapi kompleksitas teknologi modern, terutama ketika pelaku sulit diidentifikasi atau niat jahat sulit dibuktikan. Oleh karena itu, negara-negara dengan sistem hukum yang adaptif terhadap perkembangan teknologi telah berhasil memanfaatkan asas ini sebagai sarana perlindungan hukum yang kuat, khususnya bagi korban penyalahgunaan AI seperti *deepfake*.

Perkembangan teknologi kecerdasan buatan (AI) telah menciptakan peluang sekaligus tantangan baru dalam ranah hukum, salah satunya melalui kemunculan teknologi *deepfake*. *Deepfake* merupakan hasil rekayasa AI yang mampu menciptakan konten visual atau audio yang menyerupai individu nyata secara sangat realistis, bahkan sering kali tidak dapat dibedakan dengan hasil asli. Kemampuan ini menimbulkan permasalahan hukum yang kompleks, terutama ketika digunakan untuk menyesatkan publik, menyebarkan informasi palsu, atau melanggar hak privasi individu. Namun, hingga saat ini, Indonesia belum memiliki instrumen hukum yang secara eksplisit mengatur penggunaan dan penyebaran konten *deepfake* . Kekosongan hukum ini mengakibatkan lemahnya perlindungan hukum terhadap masyarakat dan rendahnya akuntabilitas penyedia teknologi AI.

Ketentuan Pasal 50 ayat (4) dalam *AI Act* Ketentuan yang mewajibkan pengungkapan (*disclosure*) atas konten yang dibuat atau dimanipulasi oleh AI sebagaimana tercantum dalam Pasal 50 ayat (4) *Artificial Intelligence Act* Uni Eropa telah menegaskan bahwa siapa pun yang menggunakan AI untuk membuat gambar, audio, atau video *deepfake*, wajib menyampaikan kepada publik bahwa konten tersebut merupakan hasil buatan atau manipulasi teknologi AI. Tujuan dari ketentuan ini adalah untuk mencegah penyesatan informasi dan pelanggaran hak individu, terutama ketika konten *deepfake* menyerupai atau menggunakan identitas seseorang tanpa sepengetahuan atau persetujuannya.

Ketentuan seperti ini belum hadir dalam sistem hukum Indonesia, dan ketidakhadirannya menciptakan celah hukum yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Selain kewajiban transparansi dalam Pasal 50, Pasal 52(3) *AI Act* juga memberikan ketentuan penting terkait klasifikasi risiko sistemik dari model AI

serbaguna. Hal ini mencerminkan pendekatan regulasi berbasis risiko *(risk-based approach)* yang lebih fleksibel dan proporsional. Di satu sisi, sistem AI yang memang berpotensi membahayakan masyarakat akan tetap diawasi ketat; namun di sisi lain, tidak semua teknologi dikenakan beban regulasi yang sama apabila dapat dibuktikan tidak menimbulkan risiko sistemik.

Dalam konteks ini, jika teknologi AI seperti *deepfake* dimanfaatkan dalam proses penegakan hukum misalnya untuk menciptakan simulasi wajah pelaku atau korban, atau untuk memprediksi risiko seseorang terhadap tindak pidana berdasarkan profil biometrik maka penggunaan tersebut berpotensi melanggar prinsip-prinsip hak asasi manusia, privasi, dan keadilan hukum apabila tidak diatur secara ketat. Ketentuan ini mencerminkan pendekatan kehati-hatian Uni Eropa terhadap penggunaan AI yang secara langsung berdampak terhadap hak-hak individu dan kebebasan sipil.

Oleh karena itu, pengaturan ketat terhadap penggunaan AI oleh lembaga penegak hukum, seperti yang diatur dalam *Annex III huruf (a) AI Act*, seharusnya menjadi rujukan normatif dalam merumuskan regulasi AI di Indonesia. Pendekatan ini akan memperkuat akuntabilitas lembaga negara, melindungi masyarakat dari potensi penyalahgunaan teknologi, serta memastikan bahwa kemajuan teknologi tidak bertentangan dengan prinsip negara hukum dan perlindungan hak asasi manusia.

Apabila ketentuan ini dibandingkan dengan kondisi di Indonesia, maka terlihat adanya kekosongan pengaturan serupa dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) maupun UU ITE. UU PDP memang mengatur prinsip kehati-hatian dan persetujuan dalam pemrosesan data pribadi, tetapi belum terdapat mekanisme klasifikasi risiko AI ataupun beban pembuktian seperti yang berlaku di Uni Eropa. Dalam konteks penyalahgunaan deepfake, ketiadaan ketentuan seperti pasal 53 AI Act dapat membuat penyedia model AI yang menghasilkan konten manipulative lepas dari tanggung jawab hukum, selama belum terbukti adanya kesalahan atau niat jahat. Namun, kerugian akibat konten deepfake seperti pelanggaran privasi, perusakan reputasi, dan penyebaran disinformasi, bersifat nyata dan luas dampaknya.

Selain langkah legislasi, Indonesia juga dapat mendorong penyusunan kode etik nasional mengenai penggunaan teknologi AI. Kode etik ini idealnya melibatkan pemangku kepentingan lintas sektor seperti Kementerian Komunikasi dan Informatika (Kominfo), Badan Riset dan Inovasi Nasional (BRIN), Badan Siber dan Sandi Negara (BSSN), serta

akademisi dan pelaku industri teknologi. Kode etik ini akan berfungsi sebagai pedoman normatif yang menjembatani kekosongan hukum formal dan mendorong perilaku bertanggung jawab dalam pengembangan dan pemanfaatan teknologi AI.

Dengan demikian, dapat disimpulkan bahwa kekosongan hukum dalam pengaturan transparansi konten *deepfake* di Indonesia perlu segera diatasi agar tidak menjadi sumber krisis sosial, etis, maupun hukum di masa depan. Adopsi prinsip-prinsip *AI Act* Uni Eropa, khususnya Pasal 50, menjadi langkah penting untuk menjamin hak masyarakat atas informasi yang akurat serta menjaga integritas ruang digital nasional. Kebijakan dalam negeri dengan standar internasional juga akan memperkuat posisi Indonesia dalam tata kelola teknologi global dan memberikan landasan hukum yang kuat untuk menghadapi tantangan era kecerdasan buatan.

Penerapan asas *strict liability* pada hukum pidana, tentunya tidak bersifat generalis atau untuk semua jenis tindak pidana, akan tetapi hanya terbatas pada tindak pidana jenis tertentu saja yang dapat diterapkan asas *strict liability*.[13] Penerapan asas *strict liability* di luar negeri terbukti lebih efektif dibandingkan di Indonesia, terutama di negara-negara yang menganut sistem hukum *common law* seperti Amerika Serikat dan Inggris. Di negara-negara tersebut, asas ini telah diterapkan secara luas dalam berbagai bidang hukum, termasuk dalam kasus-kasus yang berkaitan dengan tanggung jawab atas produk, perlindungan konsumen, hingga pelanggaran berbasis teknologi seperti penyalahgunaan kecerdasan buatan (AI) dan *deepfake*. Efektivitasnya terletak pada kemampuannya untuk menghilangkan kewajiban pembuktian unsur kesalahan (niat jahat atau kelalaian) oleh korban, sehingga proses hukum dapat berlangsung lebih cepat dan fokus pada akibat atau kerugian yang ditimbulkan.

Meskipun asas *strict liability* menawarkan kemudahan dalam pembuktian dan efektivitas penegakan hukum, penerapannya dalam sistem hukum pidana di Indonesia tidak dapat dilakukan secara menyeluruh. Hal ini disebabkan karena asas *strict liability* di Indonesia masih bersifat terbatas dan hanya diterapkan pada bidang-bidang tertentu, seperti lingkungan hidup atau perlindungan konsumen, yang diatur secara khusus dalam undang-undang sektoral. Dalam hukum pidana umum, Indonesia masih menganut asas

[13] Jalu Akbar Maulana and Fadila Nur Annisa, "*Analisa Yuridis Perubahan Makna Strict Liability dalam Undang-Undang Lingkungan Hidup Pasca Pengesahan Undang-Undang Cipta Kerja*," *Amnesti: Jurnal Hukum* 6, no. 2 (2024): 298–314.

kulpabilitas, yang mengharuskan adanya unsur kesalahan untuk dapat memidana seseorang. Oleh karena itu, penerapan asas *strict liability* dalam kasus-kasus seperti penyalahgunaan teknologi *deepfake* tidak serta-merta dapat diberlakukan tanpa terlebih dahulu melakukan reformasi terhadap kerangka hukum pidana yang berlaku.

Ketidakmungkinan penerapan asas *strict liability* dalam sistem hukum pidana Indonesia, karena keterbatasan regulasi dan asas kesalahan yang masih dominan, dapat diatasi dengan menggunakan pendekatan perbuatan melawan hukum dalam hukum pidana. Pendekatan ini memberikan alternatif untuk menjerat pelaku penyebaran *deepfake* , terutama ketika kesalahan subjektif sulit dibuktikan, namun kerugiannya nyata. Hal ini sekaligus memperlihatkan perlunya pembaruan hukum agar sistem pidana Indonesia mampu beradaptasi terhadap tantangan hukum di era digital dan kecerdasan buatan.

Sebagai langkah reformasi hukum, Indonesia perlu mempertimbangkan untuk memasukkan ketentuan mengenai pertanggungjawaban tanpa kesalahan dalam revisi Undang-Undang Perlindungan Data Pribadi, Undang-Undang ITE, maupun pembentukan undang-undang baru yang secara khusus mengatur tentang kecerdasan buatan. Selain itu, dibutuhkan keterlibatan aktif dari otoritas perlindungan data, penyedia platform digital, serta masyarakat sipil dalam membangun ekosistem hukum yang mendorong penggunaan teknologi secara bertanggung jawab dan menghormati hak privasi individu.

C. KESIMPULAN

Perkembangan teknologi *Artificial Intelligence* (AI), khususnya dalam bentuk *deepfake*, telah menimbulkan tantangan serius dalam ranah hukum, terutama terkait pertanggungjawaban atas pelanggaran privasi dan kerugian reputasi individu. Di Indonesia, meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) telah memberikan dasar perlindungan terhadap data pribadi, belum ada regulasi khusus yang mengatur secara eksplisit mengenai penggunaan AI dan konten *deepfake*. Kesulitan utama dalam penegakan hukum terhadap penyebaran *deepfake* terletak pada pembuktian unsur kesalahan, terutama karena pelaku seringkali bersifat anonim dan menggunakan teknologi yang kompleks.

Dalam konteks ini, penerapan asas *strict liability* menjadi alternatif yang relevan untuk menjawab keterbatasan hukum konvensional. Asas ini memungkinkan

pertanggungjawaban tanpa harus membuktikan adanya niat jahat atau kelalaian dari pelaku, sehingga mempermudah korban dalam memperoleh keadilan. Namun, penerapan asas *strict liability* dalam hukum pidana Indonesia masih terbatas, karena sistem hukum nasional sangat menjunjung tinggi asas kesalahan. Oleh karena itu, pendekatan perbuatan melawan hukum (PMH) dalam hukum pidana dapat dijadikan solusi sementara untuk menjerat pelaku yang menyebarkan *deepfake* meskipun tanpa bukti kesalahan subjektif.

Dibandingkan dengan Uni Eropa yang telah lebih progresif melalui AI Act dan AI *Liability Directive*, sistem hukum Indonesia masih mengalami kekosongan dalam pengaturan spesifik terhadap AI dan *deepfake*. Oleh karena itu, diperlukan langkah reformasi hukum melalui pembentukan regulasi baru, revisi UU PDP dan UU ITE, serta pembentukan lembaga pengawas independen. Dengan kerangka hukum yang lebih adaptif dan responsif, Indonesia dapat memperkuat perlindungan terhadap masyarakat di era digital dan mendorong penggunaan teknologi AI secara etis dan bertanggung jawab.

DAFTAR PUSTAKA

Buku Elektronik

Eriana, Emi Sita, and Afrizal Zein. *Artificial Intelligence (AI)*. 2023. https://repository.penerbiteureka.com/media/publications/567027-artificial-intelligence-ai-9482959d.pdf.

Jurnal Ilmiah

Adha, Lalu Adi. "Digitalisasi Industri dan Pengaruhnya terhadap Ketenagakerjaan dan Hubungan Kerja di Indonesia." *Jurnal Kompilasi Hukum*, 2020. https://jkh.unram.ac.id/index.php/jkh/article/view/49.

Santoso, Joseph Teguh. *Kecerdasan Buatan (Artificial Intelligence)*. Penerbit Yayasan Prima Agus Teknik, 2023. https://penerbit.stekom.ac.id/index.php/yayasanpat/article/download/437/465.

Maulana, Jalu Akbar, and Fadila Nur Annisa. "Analisa Yuridis Perubahan Makna Strict Liability dalam Undang-Undang Lingkungan Hidup Pasca Pengesahan Undang-Undang Cipta Kerja." *Amnesti: Jurnal Hukum* 6, no. 2 (2024): 298–314. https://jurnal.umpwr.ac.id/index.php/amnesti/article/view/4935.

Arief, Barda Nawawi. *Perbandingan Hukum Pidana*. Jakarta: Rajawali Pers, 2011.

Internet

NCC Student Activity BINUS. "Mengenal Sejarah AI & Perkembangannya." BNCC Student Activity BINUS, August 23, 2024. https://student-activity.binus.ac.id/bncc/2024/08/23/mengenal-sejarah-ai-perkembangannya/.

"Edukasi Hukum: Tindakan Deepfake." *Bullyid*. https://bullyid.org/edukasi-hukum-tindakan-deepfake/.