cek jurnal

202212005_Muh._Darayadi_Abdi_Manaf_089602306940.doc

jurnal

cek jurnal

Universitas Abdurachman Saleh

Document Details

Submission ID

trn:oid:::1:3604600853

Submission Date

Jul 1, 2026, 5:17 AM UTC

Download Date

Jul 1, 2026, 5:51 AM UTC

File Name

202212005_Muh._Darayadi_Abdi_Manaf_089602306940.doc

File Size

142.0 KB

13 Pages

4,040 Words

27,095 Characters

28% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Small Matches (less than 12 words)

Top Sources

24% Internet sources
15% Publications
23% Submitted works (Student Papers)

Integrity Flags

1 Integrity Flag for Review

Hidden Text
16 suspect characters on 12 pages
Text is altered to blend into the white background of the document.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Top Sources

24% Internet sources
15% Publications
23% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
repository.unpar.ac.id		2%
2	Student papers	
unars		2%
3	Student papers	
Universitas Jambi		1%
4	Student papers	
Tarumanagara University		1%
5	Internet	
repository.unars.ac.id		1%
6	Internet	
repository.unissula.ac.id		1%
7	Internet	
ejournal.yayasanpendidikandzurriyatulquran.id		<1%
8	Internet	
newtron21.blogspot.com		<1%
9	Student papers	
Universitas Muhammadiyah Palembang		<1%
10	Internet	
ejurnal.undana.ac.id		<1%
11	Internet	
www.ejurnal.ubk.ac.id		<1%

12 Internet

www.mkri.id <1%

13 Publication

Muhammad Reza Maulana, Agung Nugroho, Asep Suprianto. "Analisis Sentimen ... <1%

14 Student papers

Universitas Negeri Surabaya The State University of Surabaya <1%

15 Internet

jurnal.abulyatama.ac.id <1%

16 Internet

unars.ac.id <1%

17 Internet

repository.uhamka.ac.id <1%

18 Publication

Muhammad Permana Shidiq. "CHARACTERISTICS CYBER CRIME AND DYNAMICS O... <1%

19 Student papers

Fakultas Hukum <1%

20 Internet

ojs.uph.edu <1%

21 Publication

Decri Reza, Meria Utama, Henny Yuningsih. "Artificial Intelligence–Generated De... <1%

22 Internet

journal.universitaspahlawan.ac.id <1%

23 Internet

repository.upnjatim.ac.id <1%

24 Internet

www.dephub.go.id <1%

25 Internet

eprints2.ipdn.ac.id <1%

26 Internet

mimir.id <1%

27 Publication

Erlin Philein Sopaheluwakan, Teng Berlianty, Theresia Louize Pesulima. "Legal Pr... <1%

28 Internet

e-journal.unmas.ac.id <1%

29 Internet

jurnal.fh.umi.ac.id <1%

30 Internet

telset.id <1%

31 Student papers

Universitas Muhammadiyah Buton <1%

32 Internet

ejournal.unis.ac.id <1%

33 Internet

smartlegal.id <1%

34 Publication

Triani Rahmah Budiarti. "Aspek Hukum Pencantuman Kontak Darurat secara Sep... <1%

35 Student papers

UPA Perpustakaan UNTIRTA <1%

36 Student papers

Universitas Warmadewa <1%

37 Internet

ejournal.unsrat.ac.id <1%

38 Internet

ejurnals.com <1%

39 Internet

repository.unbari.ac.id <1%

40 Student papers
Universitas Diponegoro <1%

41 Internet
eprints.unimudasorong.ac.id <1%

42 Internet
journalcenter.org <1%

43 Internet
www.scribd.com <1%

44 Publication
Pupung Hermawan. "Pertanggung Jawaban Pidana Penggunaan Data Pribadi pad... <1%

45 Internet
rayyanjurnal.com <1%

46 Internet
repository.unpas.ac.id <1%

47 Student papers
Universitas Muhammadiyah Jakarta <1%

48 Internet
lama.elsam.or.id <1%

49 Internet
repository.umsu.ac.id <1%

50 Internet
www.alsa-indonesia.org <1%

Jurnal Ilmiah
FENOMENA
P-ISSN; 3047-7204, E-ISSN; 0215-1448
https://unars.ac.id/ojs/index.php/fenomena/index

PERLINDUNGAN HUKUM TERHADAP KORBAN ATAS KONTEN *DEEPFAKE* KECERDASAN BUATAN DI INDONESIA

LEGAL PROTECTION FOR VICTIMS OF ARTIFICIAL INTELLIGENCE *DEEPFAKE* CONTENT IN INDONESIA

Muh. Daryadi Abdi Manaf[1], Muhammad Yusuf Ibrahim, Rindang Gici Oktavianti[3]
[1,2,3]Ilmu Hukum, Fakultas Hukum, Universitas Abdurrachman Saleh Situbondo
Email: [1]daryabiabdi@gmail.com

Abstrak

Perkembangan teknologi kecerdasan buatan telah melahirkan teknologi *deepfake* yang mampu memanipulasi foto, video, dan suara sehingga menyerupai kondisi yang sebenarnya. Di samping memberikan manfaat, penyalahgunaan *deepfake* menimbulkan berbagai bentuk pelanggaran hukum, seperti pencemaran nama baik, penyebaran konten pornografi, penipuan, dan penyalahgunaan data pribadi yang merugikan korban secara materiil maupun immateriil. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap korban penyalahgunaan konten *deepfake* di Indonesia serta mengkaji kecukupan pengaturan hukum yang berlaku. Penelitian menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual, yang dianalisis secara deskriptif kualitatif melalui bahan hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa meskipun belum terdapat pengaturan yang secara khusus mengatur *deepfake*, perlindungan hukum terhadap korban dapat diberikan melalui Undang-Undang tentang Informasi dan Transaksi Elektronik, Undang-Undang tentang Pelindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana, serta Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Korban memiliki hak untuk memperoleh perlindungan hukum, pemulihan, penghapusan konten, penghentian pemrosesan data pribadi, dan ganti kerugian, sedangkan pelaku dapat dimintai pertanggungjawaban pidana sesuai dengan karakteristik perbuatannya. Penelitian ini menyimpulkan bahwa pengaturan hukum yang berlaku telah memberikan dasar perlindungan bagi korban penyalahgunaan *deepfake*, namun masih bersifat parsial sehingga diperlukan regulasi yang lebih spesifik mengenai kecerdasan buatan dan *deepfake* guna menjamin kepastian hukum, memperkuat perlindungan korban, dan meningkatkan efektivitas penegakan hukum di Indonesia.

Kata Kunci: perlindungan hukum, korban, *deepfake*, kecerdasan buatan, data pribadi.

Abstract

The development of artificial intelligence technology has led to the emergence of *deepfake* technology, which is capable of manipulating photographs, videos, and audio to produce highly realistic content. Despite its beneficial applications, the misuse of *deepfake* technology has given rise to various legal issues, including defamation, the dissemination of pornographic content, fraud, and the unlawful use of personal data, causing both material and immaterial harm to victims. This study aims to analyze the forms of legal protection available to victims of *deepfake* content misuse in Indonesia and to examine the adequacy of the existing legal framework. This research employs a normative legal research method using statutory and conceptual approaches, with qualitative descriptive analysis based on primary, secondary, and tertiary legal materials. The findings indicate that although Indonesian law does not yet specifically regulate *deepfake* technology, legal protection for victims may be derived from the Law on Electronic Information and Transactions, the Personal Data Protection Law, the Indonesian Criminal Code, and the Government Regulation on the Implementation of Electronic Systems and Transactions. Victims are entitled to legal protection, legal remedies, content removal, termination of personal data processing, and compensation for the losses suffered, while perpetrators may be held criminally liable according to the nature of their unlawful acts. The study concludes that the current legal framework provides a basis for protecting victims of *deepfake* misuse; however, it remains fragmented. Therefore, a more comprehensive and specific regulation on artificial intelligence and *deepfake* technology is necessary to ensure legal certainty, strengthen victim protection, and enhance the effectiveness of law enforcement in Indonesia.

Keywords: legal protection, victims, *deepfake*, artificial intelligence, personal data.

PENDAHULUAN

Kemajuan teknologi di era industri 5.0 dimanfaatkan untuk mempermudah kebutuhan manusia dalam kegiatan sehari hari. Salah satunya, *Artificial Intelegence* (selanjutnya disebut AI). AI didefinisikan sebagai cabang ilmu komputer yang berfokus pada pengembangan sistem yang dapat melakukan tugas yang biasanya memerlukan kecerdasan manusia.[1] Pemanfaatan teknologi AI dalam platform ini tidak lagi terbatas pada konten hiburan, melainkan juga mencakup representasi visual buatan. Kejahatan yang timbul dari pesatnya perkembangan teknologi mengakibatkan *cyber crime*. *Cyber crime* (kejahatan dunia maya) merupakan kejahatan yang dilakukan dengan menggunakan teknologi informasi dan komunikasi sebagai alat atau target dari kejahatan tersebut.[2] Salah satu perkembangan AI yang paling menonjol adalah teknologi *deepfake*, yaitu teknologi berbasis *deep learning* yang mampu menghasilkan atau memanipulasi gambar, video, maupun suara sehingga menyerupai identitas seseorang secara realistis. Maraknya penyalahgunaan konten *deepfake* menimbulkan berbagai dampak bagi korban, seperti pencemaran nama baik, pelanggaran privasi, kerugian ekonomi, trauma psikologis, dan eksploitasi seksual digital.[3]

Salah satu kasus penyalahgunaan *deepfake* terjadi di Gresik, di mana terdakwa mengunggah konten bermuatan melanggar kesusilaan menggunakan teknologi AI. Berdasarkan alat bukti berupa telepon genggam dan akun media sosial terdakwa, Pengadilan Negeri Gresik menyatakan terdakwa terbukti melanggar Pasal 45 ayat (1) jo. Pasal 27 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik. Dalam Putusan Nomor 265/Pid.Sus/2024/PN Gsk, terdakwa dijatuhi pidana penjara selama 1 tahun 6 bulan dan denda sebesar Rp25.000.000,00. Selain itu, penyalahgunaan *deepfake* juga terjadi dalam kasus penipuan yang menggunakan video manipulasi Prabowo Subianto dengan modus pemberian (*giveaway*) bantuan kepada masyarakat. Berdasarkan pengungkapan Tim Siber Bareskrim Polri, pelaku berinisial JS diduga telah menipu sekitar 100 korban sejak tahun 2024 dengan meminta sejumlah uang yang diklaim sebagai biaya administrasi untuk memperoleh bantuan tersebut.

Di Indonesia, hingga saat ini belum terdapat pengaturan yang secara khusus mengatur penyalahgunaan teknologi AI, khususnya *deepfake*. Penegakan hukum masih mengandalkan ketentuan yang tersebar dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Meskipun ketiga peraturan tersebut dapat digunakan sebagai dasar penegakan hukum,

[1] Moehammad Hikal Pratama *Et.Al,* 2024, *Kecerdasan Buatan Dalam Transformasi Digital: Peluang Dan Tantangan Modern*, Pustaka Galeri Mandiri, Vol.4, No.3, Hal.79-83.

[2] Rian Dwi Hapsari, Kuncoro Galih Pambayun, 2023, *Ancaman Cybercime di Indonesia,* Jurnal Konstituen, Vol, No.1, Hal.7.

[3] Ni Putu Martina Putri, *Et.Al*, 2024, *Analisis Reformulasi Pertanggung Jawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelegence,* Jurnal Pacta Sunt Servanda, Vol.5, No.2, Hal.125.

pengaturannya masih bersifat parsial sehingga belum mampu mengakomodasi karakteristik kejahatan *deepfake* secara komprehensif. Akibatnya, perlindungan hukum terhadap korban masih menghadapi berbagai kendala, baik dalam aspek kepastian hukum, pembuktian, maupun pemulihan hak-hak korban.

Penelitian mengenai *deepfake* telah banyak dilakukan. Rendi Syaputra Nur Haida dan Eko Nuriyatman menyoroti urgensi pembentukan regulasi khusus terhadap penyalahgunaan *deepfake*. Musfala Yudha dkk. mengkaji perlindungan hukum korban *deepfake* dalam kejahatan pornografi, sedangkan Ardhia Pramesti Regita Putri dan Nuri Hidayati membahas strategi penguatan perlindungan hukum melalui pembentukan regulasi yang lebih komprehensif. Sementara itu, Rizgita Nurul Fauzyah dkk. menekankan pentingnya pengaturan khusus mengenai AI dalam memberikan perlindungan hukum terhadap korban *deepfake porn* di Indonesia.

Berbeda dengan penelitian sebelumnya, penelitian ini mengkaji perlindungan hukum terhadap korban penyalahgunaan konten *deepfake* secara komprehensif, tidak hanya terbatas pada kasus pornografi, tetapi juga pencemaran nama baik, penipuan, penyalahgunaan data pribadi, dan pelanggaran hak privasi. Penelitian ini bertujuan menganalisis bentuk perlindungan hukum bagi korban serta menilai kecukupan pengaturan dalam UU ITE, UU Perlindungan Data Pribadi, dan KUHP dalam memberikan kepastian hukum dan perlindungan terhadap korban penyalahgunaan *deepfake* di Indonesia. Berdasarkan latar belakang diatas, maka penulis tertarik untuk mengkaji penelitian ini yang berjudul "Perlindungan Hukum Terhadap Korban Atas Konten Kecerdasan Buatan di Indonesia".

METODE PENELITIAN

Metode penelitian dalam penulisan jurnal ini dengan menggunakan jenis penelitian hukum yuridis normatif (doctrinal research) yaitu penelitian yang berdasarkan pada kepustakaan yang berfokus pada analisis bahan hukum primer dan bahan hukum sekunder serta bahan hukum lainnya yang dapat mendukung penulisan jurnal ini. Peneliti dalam tulisan ini menerapkan dua model pendekatan penelitian yakni pendekatan perundang-undangan (*statue aproach)* dan pendekatan konseptual (*conceptual aproach)*. Pendekatan peraturan perundang-undangan (*statute approach*) adalah pendekatan yang dilakukan untuk menelaah isu hukum yang dijadikan pokok pembahasan yang ditelaah atau dikaji dengan menggunakan semua peraturan perundang-undangan dan regulasi yang berkaitan dengan udang-undang tertentu.[4] Selanjutnya, pendekatan yang kedua yakni Pendekatan konseptual (*conceptual aproach)* adalah pendekatan yang dilaksanakan jika suatu penelitian tidak berpindah dari suatu aturan yang berlaku, Pedekatan ini merujuk pada prinsip-prinsip yang ditemukan dalam perspektif ahli hukum atau doktrin-doktrin hukum yang ada.[5]

[4] Muhammad Yusuf Ibrahim, 2023, *Karakteristik Rahasia Dagang Sebagai Hak Kebendaan*, Basnish Publishing, Situbondo, Hal.99.

[5] *Ibid*, Hal. 100.

HASIL DAN PEMBAHASAN

1. Perlindungan Hukum Terhadap Korban Atas Konten *Deepfake* Kecerdasan Buatan di Indonesia

Kemajuan teknologi pada era Industri 5.0 telah mempermudah berbagai aktivitas manusia sekaligus mengubah cara berpikir, bekerja, dan berinteraksi. Salah satunya AI, AI merupakan suatu sistem yang dikembangkan dan mampu berinovasi dalam bidang studi yang dimodelkan baik pada mesin maupun komputer yang dapat memiliki kecerdasan yang sama atau bahkan lebih dari manusia.[6] AI seringkali digunakan oleh manusia sebagai alat bantu penunjang pekerjaan manusia mencakup kemampuan untuk belajar dari data (selayaknya manusia belajar dari pengalaman), memahami, bahasa alami, menggali pola, dan membuat keputusan.[7] Perkembangan teknologi AI telah melahirkan berbagai bentuk konten digital manipulatif, seperti *deepfake*, penggandaan suara, manipulasi foto dan video, pornografi berbasis AI, penyebaran informasi palsu, serta penyamaran identitas digital. Maraknya fenomena konten tersebut membawa dampak destruktif yang sangat nyata bagi korbannya, yang meliputi kerugian moral, pencemaran nama baik, pelanggaran privasi yang masif, kerugian ekonomi akibat penipuan berbasis identitas, trauma psikologis yang mendalam, hingga ancaman eksploitasi seksual digital.[8]

Dasar filosofis perlindungan hukum terhadap korban penyalahgunaan AI berlandaskan Pasal 1 ayat (3) UUD 1945 yang menegaskan Indonesia sebagai negara hukum. Oleh karena itu, negara berkewajiban menjamin perlindungan hak asasi manusia melalui kepastian hukum, keadilan, dan kemanfaatan hukum. Jaminan tersebut dipertegas dalam Pasal 28D ayat (1) dan Pasal 28G ayat (1) UUD 1945 yang mengatur hak atas kepastian hukum, perlindungan diri, kehormatan, martabat, harta benda, dan rasa aman. Menurut Philipus M. Hadjon, perlindungan hukum merupakan upaya melindungi hak asasi manusia serta harkat dan martabat setiap subjek hukum dari tindakan sewenang-wenang berdasarkan ketentuan hukum.[9] Philipus M. Hadjon membagi perlindungan hukum menjadi dua bentuk, yaitu perlindungan preventif yang bertujuan mencegah terjadinya sengketa, dan perlindungan represif yang berfungsi menyelesaikan sengketa setelah terjadi pelanggaran hukum melalui pengadilan atau lembaga penyelesaian sengketa lainnya.[10]

Perkembangan AI telah melahirkan berbagai inovasi, salah satunya *deepfake*, yang berpotensi menimbulkan korban di ruang siber. *Deepfake* merupakan hasil manipulasi digital berbasis *deep learning* yang menghasilkan foto, video, atau audio realistis sehingga seolah-olah seseorang mengatakan atau

---

[6] Moehammad Hikal Pratama, *Et.Al, Loc.Cit.*

[7] Sudirwo, *Et.Al*, *Artificial Integence (Teori,Konsep, Dan Impplementasi Di Berbagi Bidang)*, Sonpedia Publishig, Jambi, Hal.1.

[8] Ni Putu Martina Putri, *Et.Al*, *Loc.Cit.*

[9] Muhammad Yusuf Ibrahim, *Op.Cit,* Hal.31.

[10] *Ibid,* Hal.31-32.

melakukan sesuatu yang sebenarnya tidak pernah terjadi.[11] Teknologi ini pada dasarnya menggunakan algoritma kompleks untuk mereplikasi pola wajah dan menganalisis, gerakan, serta suara dari data asli yang tersedia, lalu menghasilkan konten tiruan yang nyaris sulit terdeteksi oleh pengamat biasa.[12] Pada mulanya, teknologi *deepfake* lebih banyak dimanfaatkan untuk keperluan hiburan, seperti melakukan pertukaran wajah (*face swap*) pada aktor dalam film atau menciptakan karakter fiktif yang tampak realistis. Akan tetapi, seiring dengan pesatnya perkembangan teknologi tersebut, penggunaannya semakin meluas hingga memasuki bidang yang lebih kompleks dan sensitif, termasuk politik, hukum, serta berbagai bentuk kejahatan siber.[13]

Selama ini yang menjadi rujukan atau landasan hukum pengaturan mengenai penyalahgunaan teknologi khususnya *cyber crime*, masih bertumpu pada UU ITE. Meskipun belum mengatur AI secara khusus, AI dapat dikualifikasikan sebagai Agen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 8 UU ITE, yaitu perangkat dalam sistem elektronik yang mampu menjalankan tindakan terhadap informasi elektronik secara otomatis. Karakteristik tersebut sejalan dengan kemampuan AI dalam mengolah data, mengenali pola, dan menghasilkan keputusan berdasarkan algoritma.[14] Selain itu, Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial mendefinisikan AI sebagai sistem yang mampu melakukan pemrosesan dan pengelolaan data secara cermat, sedangkan pihak yang mengembangkan atau mengoperasikan sistem AI dapat dikategorikan sebagai Penyelenggara Sistem Elektronik sesuai ketentuan peraturan perundang-undangan. Dalam konteks penyalahgunaan *deepfake*, UU ITE menyediakan dasar hukum melalui Pasal 27 ayat (1) mengenai distribusi konten yang melanggar kesusilaan, Pasal 27A mengenai pencemaran nama baik, Pasal 28 ayat (1) mengenai penyebaran informasi bohong yang menimbulkan kerugian materiil, serta Pasal 35 mengenai larangan melakukan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik agar seolah-olah merupakan data yang autentik. Oleh karena itu, pembuatan maupun penyebaran konten *deepfake* yang merekayasa wajah, suara, atau identitas seseorang pada dasarnya dapat memenuhi unsur tindak pidana sebagaimana diatur dalam ketentuan-ketentuan tersebut, meskipun hingga kini belum terdapat pengaturan yang secara khusus mengatur teknologi *deepfake*. *Deepfake* pada umumnya menitikberatkan pada manipulasi data pribadi yang bersifat seksual dengan memanfaatkan teknologi untuk merekayasa identitas atau citra seseorang. Kejahatan ini dilakukan melalui penggunaan teknologi digital dalam proses pembuatannya dan

[11] Indri Kurnia Andani, 2025, *Pertanggung Jawaban Pidana Deepfake Mengandung Unsur Pornografi Melalui Artificial Intelgence (Ai), Skripsi,* Program Studi Ilmu Hukum Universitas Borneo Tarakan: Borneo, Hal.22.

[12] Ni Putu Martina Putri, *Et.Al*, *Op.Cit.* Hal.124.

[13] *Ibid*.

[14] Andhika Nugraha *Et.Al*, 2023, *Analisis Hukum Terhadap Upaya Pencegahan Kasus Deeofake Porn Dan Pendidikan Kesadaran Publik Di Lingkungan Digital,* Jurnal Pendidikan Tambusai, Vol.7, No.2, Hal.26182.

kemudian disebarluaskan melalui berbagai platform atau media digital, sehingga berpotensi menimbulkan kerugian bagi korban baik secara pribadi maupun sosial.[15]

Perlindungan hukum terhadap korban *deepfake* juga diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Pasal 20 mewajibkan setiap pemrosesan data pribadi didasarkan pada persetujuan yang sah atau dasar hukum lainnya, sedangkan Pasal 29 mengharuskan pengendali data menjamin akurasi, kelengkapan, dan konsistensi data melalui proses verifikasi. Selain itu, Pasal 65 ayat (1) dan ayat (3) melarang setiap orang memperoleh maupun menggunakan data pribadi milik orang lain secara melawan hukum. UU PDP juga mengakui data biometrik, seperti wajah dan suara, sebagai data pribadi yang bersifat spesifik sehingga penggunaannya untuk membuat konten *deepfake* tanpa persetujuan pemilik data dapat dikategorikan sebagai pelanggaran terhadap hak atas data pribadi. Oleh karena itu, pemanfaatan foto, video, atau rekaman suara seseorang dalam pembuatan konten berbasis AI tanpa persetujuan yang sah berpotensi melanggar ketentuan UU PDP.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) dapat menjadi dasar hukum dalam memberikan perlindungan terhadap korban penyalahgunaan *Artificial Intelligence* (AI), khususnya *deepfake*. Ketentuan yang relevan meliputi Pasal 332 ayat (2) dan (3) mengenai akses ilegal terhadap sistem elektronik, Pasal 407 tentang pornografi, Pasal 433 tentang pencemaran nama baik, serta Pasal 482 dan Pasal 483 mengenai pemerasan dan pengancaman. Dengan demikian, penyalahgunaan *deepfake* yang melibatkan manipulasi identitas, penyebaran konten pornografi, pencemaran nama baik, atau pemerasan dapat dijerat menggunakan ketentuan-ketentuan tersebut.

Perlindungan hukum terhadap korban penyalahgunaan *Artificial Intelligence* (AI) memerlukan penerapan berbagai instrumen hukum karena tidak dapat bergantung pada satu peraturan saja. Meskipun Indonesia telah memiliki UU ITE, UU Pelindungan Data Pribadi, dan KUHP, pelaksanaannya masih menghadapi sejumlah hambatan, antara lain perkembangan AI yang lebih cepat daripada pembentukan regulasi, rendahnya literasi digital masyarakat, sulitnya mengidentifikasi pelaku yang beroperasi secara anonim dan lintas negara, serta belum optimalnya pengawasan dan koordinasi antarlembaga. Kondisi tersebut menyebabkan perlindungan hukum terhadap korban penyalahgunaan konten AI belum terlaksana secara efektif.

2. Akibat Hukum Atas Konten *Deepfake* Kecerdasan Buatan di Indonesia

Deepfake merupakan teknologi berbasis *deep learning* yang mampu memanipulasi foto, suara, atau video sehingga menghasilkan konten yang tampak autentik.[16] Namun, teknologi ini kerap disalahgunakan untuk penyebaran

[15] Novyanti, Heny, 2022, *Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana*, Jurnal Unesa 1, Vol.9, No. 04, 202, Hal.2.

[16] Indri Kurnia Andani, *Loc,Cit.*

disinformasi, pencemaran nama baik, dan pelecehan seksual berbasis digital. Penggunaan identitas biometrik seseorang tanpa persetujuan dapat menimbulkan kerugian materiil maupun immateriil bagi korban.[17] Oleh karena itu, diperlukan analisis mengenai akibat hukum yang timbul serta bentuk perlindungan hukum bagi korban penyalahgunaan konten *deepfake*.

Akibat hukum pada dasarnya merupakan konsekuensi yang ditimbulkan oleh suatu peristiwa hukum atau perbuatan hukum yang menimbulkan hak dan kewajiban bagi subjek hukum.[18] Menurut Soedjono Dirjosisworo, akibat hukum merupakan akibat yang ditimbulkan oleh hubungan hukum yang melahirkan hak dan kewajiban bagi para pihak yang terlibat.[19] Dalam penyalahgunaan *deepfake*, akibat hukum tidak hanya berupa pertanggungjawaban yang dibebankan kepada pelaku, tetapi juga memberikan hak kepada korban untuk memperoleh perlindungan hukum, pemulihan, serta ganti kerugian atas kerugian yang ditimbulkan. Dalam praktiknya, pembuatan konten *deepfake* umumnya memanfaatkan foto, video, suara, maupun data biometrik seseorang yang diperoleh dari media sosial atau sumber digital lainnya tanpa persetujuan pemilik data.[20]

UU ITE sebagaimana telah diubah untuk kedua kalinya pada tahun 2024 berperan sebagai instrumen hukum yang relevan dalam mengatur dan menanggulangi penyalahgunaan teknologi *deepfake* di Indonesia. Meskipun belum mengatur *deepfake* secara khusus, ketentuan dalam undang-undang tersebut dapat ditafsirkan dan diterapkan terhadap berbagai bentuk penyalahgunaan teknologi kecerdasan buatan yang melibatkan manipulasi informasi maupun konten digital.[21]Meskipun tidak mengatur *deepfake* secara khusus, UU ITE dapat diterapkan terhadap penyalahgunaannya. Pasal 27A UU ITE melarang pendistribusian atau penyebaran informasi elektronik yang menyerang kehormatan atau nama baik seseorang, sehingga pelaku yang menggunakan *deepfake* untuk pencemaran nama baik dapat dipidana berdasarkan Pasal 45 ayat (4) dengan ancaman pidana paling lama 2 tahun dan/atau denda paling banyak Rp400.000.000,00. Selain digunakan untuk pencemaran nama baik teknologi *deepfake* juga seringkali digunakan untuk membuat konten pornografi dengan cara menempelkan wajah atau identitas seseorang kedalam foto maupun video yang mengandung muatan seksual tanpa adanya persetujuan korban.[22] *deepfake* yang digunakan untuk membuat dan menyebarkan konten pornografi tanpa persetujuan korban dapat dijerat Pasal 27 ayat (1) UU ITE. Berdasarkan Pasal 45 ayat (1), pelaku diancam pidana penjara paling lama 6 tahun dan/atau denda

[17] Gunawan Widjaja, 2025, *Deepfake Dan Masa Depan Kebenaran: Implikasi Etis Dan Sosisial,* Berajah Journal, Vol.5, No.2, Hal.148.

[18] Moeljatno 2015, *Asas-Asas Hukum Pidana*, Rineka Cipta: Jakarta, Hal.1.

[19] Soejono Disworo *Loc.Cit.*

[20] Gunawan Widjaja *Op.Cit,* Hal.151.

[21] *Ibid,* Hal.160.

[22] Carens Amanda Gea Pitaloka, 2025, *Penyalahgunaan Teknologi Deepfake Untuk Konten Pornografi Non-Konsesual Di Indonesia,* Jurnal Hukum Sosial Dan Humaniora, Vol.2, No.2, Hal.77.

paling banyak Rp1.000.000.000,00. Akibat hukum bagi korban penyalahgunaan *deepfake* meliputi hak untuk mengajukan keberatan atas penggunaan data pribadinya, meminta penghapusan data yang digunakan secara melawan hukum, serta menuntut pelaku sesuai ketentuan peraturan perundang-undangan. Hak tersebut sejalan dengan Pasal 15 Peraturan Pemerintah Penyelenggara Sistem dan Transaksi Elektronik yang mengatur mekanisme penghapusan (*right to erasure)* dan pengeluaran dari daftar mesin pencaarian (*right to delisting)* terhadap informasi elektronik yang tidak relevan.

Dalam UU PDP memberikan perlindungan terhadap data biometrik, seperti wajah dan suara, yang sering disalahgunakan dalam pembuatan *deepfake*. Berdasarkan Pasal 4, data biometrik merupakan data pribadi yang bersifat spesifik, sehingga pemrosesannya harus didasarkan pada persetujuan yang sah dari subjek data sebagaimana diatur dalam Pasal 20 ayat (2) huruf a. Apabila data biometrik digunakan tanpa persetujuan, korban berhak memperoleh perlindungan sebagaimana diatur dalam Bab IV UU PDP, termasuk hak untuk mengakses, memperbaiki, menghentikan pemrosesan, menarik persetujuan, meminta penghapusan data, serta menuntut ganti rugi atas pelanggaran pemrosesan data pribadi berdasarkan Pasal 12.Di sisi lain, UU PDP juga mengatur pertanggungjawaban pidana bagi pelaku. Pasal 65 melarang memperoleh, mengungkapkan, dan menggunakan data pribadi milik orang lain secara melawan hukum, sedangkan sanksi pidananya diatur dalam Pasal 67 dengan ancaman pidana penjara hingga 5 tahun dan/atau denda paling banyak Rp5 miliar. Ketentuan tersebut dapat diterapkan terhadap pelaku yang menggunakan data biometrik seseorang untuk membuat atau menyebarkan konten *deepfake* tanpa persetujuan pemilik data.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) dapat menjadi dasar hukum dalam menindak penyalahgunaan teknologi *deepfake*, meskipun belum mengaturnya secara khusus. Pasal 332 ayat (2) dan (3) mengatur tindak pidana akses ilegal terhadap sistem elektronik dengan ancaman pidana penjara paling lama 7 tahun atau 8 tahun, tergantung bentuk perbuatannya. Selain itu, penyebaran *deepfake* bermuatan pornografi dapat dijerat Pasal 407 dengan ancaman pidana penjara paling lama 10 tahun atau denda kategori VI. Apabila *deepfake* digunakan untuk menyerang kehormatan atau nama baik seseorang, pelaku dapat dikenakan Pasal 433 ayat (2) dengan ancaman pidana penjara paling lama 1 tahun 6 bulan atau denda kategori III. Sementara itu, penggunaan *deepfake* sebagai sarana pemerasan atau pengancaman dapat dikenakan Pasal 482 dan Pasal 483 KUHP dengan ancaman pidana penjara paling lama 9 tahun atau 4 tahun. Dengan demikian, meskipun belum terdapat pengaturan khusus mengenai *deepfake*, KUHP 2023 telah menyediakan dasar hukum untuk menindak berbagai bentuk penyalahgunaannya.

Dalam perspektif UU PDP, penggunaan wajah, suara, atau data biometrik lainnya untuk membuat konten *deepfake* tanpa persetujuan merupakan pelanggaran pemrosesan data pribadi. Korban berhak memperoleh perlindungan, meminta penghapusan data, serta menuntut ganti rugi, sedangkan pelaku dapat

dikenai sanksi berdasarkan Pasal 65 jo. Pasal 67 UU PDP. Sementara itu, UU ITE dapat diterapkan terhadap *deepfake* yang digunakan untuk pencemaran nama baik maupun penyebaran konten pornografi melalui Pasal 27A jo. Pasal 45 ayat (4) dan Pasal 27 ayat (1) jo. Pasal 45 ayat (1), serta memberikan hak kepada korban untuk mengajukan *right to erasure* dan *right to delisting*. Selain itu, KUHP 2023 melengkapi perlindungan hukum melalui pengaturan mengenai akses ilegal, pencemaran nama baik, pornografi, pemerasan, dan pengancaman. Dengan demikian, meskipun belum terdapat regulasi khusus mengenai *deepfake*, kombinasi pengaturan dalam UU PDP, UU ITE, dan KUHP 2023 telah menjadi dasar hukum dalam melindungi korban dan menindak pelaku. Namun, pengaturan yang lebih spesifik tetap diperlukan untuk memberikan kepastian hukum dan meningkatkan efektivitas penegakan hukum di Indonesia.

PENUTUP

Perlindungan hukum terhadap korban atas konten *deepfake* kecerdasan buatan di Indonesia diatur pada ketentuan UU ITE. Pasal 27A UU ITE mengatur tentang pencemaran nama baik, Pasal 27 ayat (1) mengatur pelarangan konten yang melanggar keasusilaan, Pasal 28 ayat (1) mengatur pelarangan berita bohong dan informasi menyesatkan. Pasal 65 ayat (1) dan ayat (3) UU PDP mengatur larangan penggunaan data pribadi secara melawan hukum memperoleh data pribadi yang bukan miliknya. Hak korban diatur dalam Pasal 3 PP PSTE yang dimana penyelenggara sistem elektronik harus dilakukan secara andal, aman, dan bertanggung jawab. Pasal 15 PP PSTE mengatur perihal penghapusan informasi elektronik yang tidak relevan melalui mekanisme (*right to erasure)* dan pengeluaran dari daftar mesin pencari (*right to delisting)*. Pasal 16 PP PSTE mengatur mengenai mekanisme penghapusan informasi elektronik. Selanjutnya, dalam KUHP 2023 Pasal 332 ayat (2) dan (3) menjelaskan tindak pidana terhadap informatika dan elektronika. Pasal 407 menjelaskan tentang pornografi. Pasal 433 tentang pencemaran nama baik atau kehormatan orang lain. Pasal 482 dan 483 mengatur tentang tindak pidana pemerasan dan pengancaman.

Akibat hukum dalam UU ITE diatur dalam Pasal 45 ayat (4) UU ITE memberikan ancaman pidana penjara paling lama 2 (dua) Tahun dan/atau denda paling banyak Rp 400.000.000,00 (empat ratus juta rupiah). Akibat hukum Pasal 45 ayat (1) UU ITE dipidana penjara paling lama 6 (enam) tahun dan /atau denda pidana paling banyak Rp 1 (satu) miliar. Dalam UU PDP Akibat hukum diatur dalam Pasal 67 UU PDP dengan ancaman paling lama 5 (lima) tahun dan denda/atau denda paling banyak Rp 5 (lima) miliar, untuk pelanggaran Pasal 65 ayat (1) pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp 4 (empat) miliar untuk pelanggaran Pasal 65 ayat (2), selanjutnya pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp 5 (lima) miliar untuk pelanggaran Pasal 65 ayat (3). Akibat hukum dalam Pasal 332 ayat (2) KUHP 2023 dipidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori V Rp 500.000.000,00 (limaratus juta rupiah). Akibat hukum Pasal 332 ayat (3) dipidana penjara paling lama 8 (delapan) tahun atau pidana

denda paling banyak kategori VI Rp 2 (dua) miliar. Akibat hukum Pasal 407 dipidana penjara paling lama 10 (sepuluh) tahun atau denda paling banyak kategori VI Rp 2 (dua) miliar. Akibat hukum Pasal 433 ayat (2) dipidana penjara paling lama 1 (satu) tahun 6 (enam) bulan atau pidana denda paling banyak kategori III Rp 50.000.000,00 (limah puluh juta rupiah). Akibat hukum Pasal 482 pelaku pemerasan dapat dipidana penjara paling lama 9 (sembilan) tahun. Akibat hukum yang timbul pada Pasal 483 pelaku dapat dipidana penjara paling lama 4 (empat) tahun atau pidana denda baling banyak kategori IV Rp 200.000.000,00 (dua ratus juta rupiah).

Berdasarkan kesimpulan diatas, penulis mengajukan saran-saran sebagai berikut:

1. Kepada DPR selaku pembentuk undang-undang, perlu membentuk regulasi khusus mengenai kecerdasan buatan, terutama terkait konten *deepfake*, yang memuat definisi, batasan penggunaan, mekanisme pengawasan, serta pertanggungjawaban hukum. Selain itu, diperlukan penguatan koordinasi dengan penyelenggara sistem elektronik dan platform digital dalam mendeteksi, membatasi, dan menghapus konten *deepfake* yang merugikan korban.
2. Kepada praktisi hukum advokat, jaksa, penyidik, maupun konsultan hukum, diharapkan dapat meningkatkan kapasitas dan pemahaman mengenai perkembangan teknologi kecerdasan buatan, khususnya terkait karakteristik, modus operandi, serta dampak hukum dari konten deepfake. Peningkatan kompetensi ini penting untuk mendukung proses penanganan perkara secara efektif, mulai dari identifikasi unsur pelanggaran, pengumpulan dan analisis alat bukti elektronik, hingga pendampingan hukum bagi korban.
3. Kepada masyarakat, perlu meningkatkan literasi digital dan pemahaman mengenai risiko penyalahgunaan teknologi kecerdasan buatan, khususnya *deepfake*. Sikap kritis terhadap informasi, gambar, video, maupun rekaman suara yang beredar di media digital sangat diperlukan untuk mencegah penyebaran konten manipulatif yang dapat merugikan pihak lain. Selain itu, masyarakat yang menjadi korban penyalahgunaan deepfake hendaknya segera memanfaatkan mekanisme hukum yang tersedia dengan melaporkan perbuatan tersebut kepada aparat penegak hukum atau instansi terkait agar memperoleh perlindungan dan pemulihan hak sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

DAFTAR PUSTAKA

Buku

Muhammad Yusuf Ibrahim, 2023, *Karakteristik Rahasia Dagang Sebagai Hak Kebendaan*, Basnish Publishing, Situbondo.

Moeljatno 2015, *Asas-Asas Hukum Pidana*, Rineka Cipta: Jakarta.

Sudirwo, *Et.Al*, *Artificial Integence (Teori,Konsep, Dan Impplementasi Di Berbagi Bidang)*, Sonpedia Publishig, Jambi.

Skripsi

Indri Kurnia Andani, 2025, *Pertanggung Jawaban Pidana Deepfake Mengandung Unsur Pornografi Melalui Artificial Intelgence (Ai), Skripsi,* Program Studi Ilmu Hukum Universitas Borneo Tarakan: Borneo.

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2019 Tentang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang No 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

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

Undang-Undang RI Nomor 1 Tahun 2023 Kitab Undang Undang Hukum Pidana.

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Surat Edaran Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 9 Tahun 2023 Tentang Etika Kecerdasan Artifisial.

Jurnal

Andhika Nugraha *Et.Al*, 2023, *Analisis Hukum Terhadap Upaya Pencegahan Kasus Deeofake Porn Dan Pendidikan Kesadaran Publik Di Lingkungan Digital,* Jurnal Pendidikan Tambusai, Vol.7, No.2.

Carens Amanda Gea Pitaloka, 2025, *Penyalahgunaan Teknologi Deepfake Untuk Konten Pornografi Non-Konsesual Di Indonesia,* Jurnal Hukum Sosial Dan Humaniora, Vol.2, No.2.

Gunawan Widjaja, 2025, *Deepfake Dan Masa Depan Kebenaran: Implikasi Etis Dan Sosisial,* Berajah Journal, Vol.5, No.2.

Moehammad Hikal Pratama *Et.Al,* 2024, *Kecerdasan Buatan Dalam Transformasi Digital: Peluang Dan Tantangan Modern*, Pustaka Galeri Mandiri, Vol.4, No.3.

Ni Putu Martina Putri, *Et.Al*, 2024, *Analisis Reformulasi Pertanggung Jawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelegence,* Jurnal Pacta Sunt Servanda, Vol.5, No.2.

Novyanti, Heny, 2022, *Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana*, Jurnal Unesa 1, Vol.9, No. 04, 202.

Rian Dwi Hapsari, Kuncoro Galih Pambayun, 2023, *Ancaman Cybercime di Indonesia,* Jurnal Konstituen, Vol, No.1, Hal.7.